



TSM-39

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: T. TERAMURA, et al

Serial No.: 10/811,905

Filed: March 30, 2004

For: ELECTRONIC KEY SYSTEM AND ELECTRONIC KEY USAGE METHOD

Group: 2635

Examiner: W. L. Bangachon

**LETTER CLAIMING RIGHT OF PRIORITY**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

April 11, 2006

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, applicants hereby claim  
the right of priority based on:

**Japanese Application No. 2003-118126**  
**Filed: April 23, 2003**

A Certified copy of said application document is attached hereto.

Respectfully submitted,

\_\_\_\_\_  
Carl I. Brundidge  
Registration No. 29,621  
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

CIB/jdc  
Enclosures  
703/684-1120



## JAPAN PATENT OFFICE

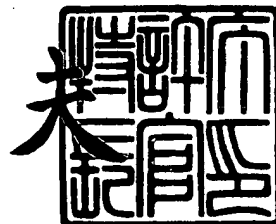
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 人 株式会社日立製作所  
Applicant(s):

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

**BEST AVAILABLE COPY**

今井康



【書類名】 特許願

【整理番号】 HK14920000

【提出日】 平成15年 4月23日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 寺村 健

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 齊藤 元伸

【発明者】

【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 情報・通信グループ内

【氏名】 桑名 利幸

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100084032

【弁理士】

【氏名又は名称】 三品 岩男

【電話番号】 045(316)3711

【手数料の表示】

【予納台帳番号】 011992

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

**【書類名】 明細書****【発明の名称】 電子鍵システムおよび電子鍵利用方法****【特許請求の範囲】****【請求項 1】**

電子鍵を利用してサービス提供を行う電子鍵システムにおいて、

電子鍵を識別するための主 ID および副 ID を有する電子鍵データを記憶した利用者モジュールと、サービス提供可否を判定するサービス提供デバイスとを有し、

前記利用者モジュールは、サービス提供デバイスからの電子鍵の送信要求を受け付ける受付手段と、電子鍵データを前記サービス提供デバイスに送信する送信手段を有し、

前記サービス提供デバイスは、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、利用者モジュールから電子鍵データを受け付ける受付手段と、前記受け付けた電子鍵データの主 ID が、前記サービス許可情報に存在するか否かを判定する第 1 の判定手段と、前記受け付けた電子鍵データの副 ID が、前記サービス拒否情報に存在するか否かを判定する第 2 の判定手段とを有し、

前記サービス提供デバイスは、前記第 1 および第 2 の判定結果により、サービス提供可否を判断する提供判断手段とを有すること、

を特徴とする電子鍵システム。

**【請求項 2】**

請求項 1 に記載の電子鍵システムにおいて、

前記提供判断手段は、前記第 1 の判定手段において、主 ID が前記サービス許可テーブルに存在すると判定し、かつ、前記第 2 の判定手段において、副 ID が前記サービス拒否テーブルに存在しない場合に、サービス提供を許可すること  
を特徴とする電子鍵システム。

**【請求項 3】**

請求項 1 または 2 に記載の電子鍵システムにおいて、

前記電子鍵データは、電子鍵の共有可能か否かを示す共有階層データを有し、

前記利用者モジュールは、共有階層データが共有可能な場合に、主 I D が同一で、かつ副 I D が異なる共有用電子鍵を生成する生成手段を有することを特徴とする電子鍵システム。

**【請求項 4】**

請求項 1、2 または 3 に記載の電子鍵システムにおいて、

前記電子鍵システムは、電子鍵サービスを管理する電子鍵管理装置を有し、

前記電子鍵管理装置は、利用者を識別する会員番号と副 I D を含む顧客テーブルを記憶する手段と、外部システムから会員番号および副 I D を受け付ける受付手段と、受け付けた会員番号に対応する前記顧客テーブルの副 I D と、受け付けた副 I D とが一致するか否かを判定し、前記判定手段に基づき、同一の主 I D を有する利用者モジュールを全て無効化する全体無効化処理を行うか、または、同一の副 I D を有する利用者モジュールのみを無効化する部分無効化処理を行うかを判定する無効化判定手段と、前記無効化判定結果を前記サービス提供デバイスに送信する送信手段とを有し、

前記サービス提供デバイスは、前記無効化判定結果に応じて、サービス拒否テーブルまたはサービス許可テーブルの変更を行う変更手段を有すること

を特徴とする電子鍵システム。

**【請求項 5】**

サービス提供を行うサービス提供デバイスが、サービス提供可否を判定するために用いる電子鍵データを記憶した利用者モジュールにおいて、

前記電子鍵データは、電子鍵を識別するための主 I D データおよび副 I D データを有し、

前記利用者モジュールは、前記サービス提供デバイスから電子鍵の送信要求を受け付ける送信要求受付手段と、電子鍵データを前記サービス提供デバイスに送信する送信手段とを有すること

を特徴とする利用者モジュール。

**【請求項 6】**

請求項 5 に記載の利用者モジュールにおいて、

前記電子鍵データは、電子鍵の共有可能なか否かを示す共有階層データを有し、

前記利用者モジュールは、電子鍵の共有要求を受け付ける共有要求受付手段と、

共有可能な場合に、主 I D が同一で、かつ副 I D が異なる共有用電子鍵データを生成する生成手段と、

前記生成した共有用電子鍵データを、外部システムに送信する送信手段とを有すること

を特徴とする利用者モジュール。

#### 【請求項 7】

請求項 6 に記載の利用者モジュールにおいて、

前記利用者モジュールは、共有階層データが所定の値の場合は共有不可と判断し、共有階層データの値が所定の値以外の場合は共有可能と判定する共有判断手段とを有し、

前記生成手段は、電子鍵データの共有階層データの値を「1」減算した値に変更して共有用電子鍵データを生成すること

を特徴とする利用者モジュール。

#### 【請求項 8】

利用者モジュールに記憶された電子鍵データを利用し、サービス提供可否を判定するサービス提供デバイスにおいて、

サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、

利用者モジュールから電子鍵データを受け付ける受付手段と、

前記受け付けた電子鍵データと、前記サービス許可情報と、前記サービス拒否情報とにものとづき、前記受け付けた電子鍵データのサービス提供可否を判断する判断手段と、を有すること、

を特徴とするサービス提供デバイス。

#### 【請求項 9】

請求項 8 に記載のサービス提供デバイスであって、

前記電子鍵データは、電子鍵を識別するための主 I D データおよび副 I D データを有し、

前記判断手段は、前記受け付けた電子鍵データの主 I D が、前記サービス許可情報に存在するか否かを判定する第 1 の判定手段と、前記受け付けた電子鍵データの副 I D が、前記サービス拒否情報に存在するか否かを判定する第 2 の判定手段とを有し、前記第 1 および第 2 の判定結果に応じて、前記受け付けた電子鍵データのサービス提供可否を判断すること、

を特徴とするサービス提供デバイス。

#### 【請求項 1 0】

利用者モジュールに記憶された電子鍵データを利用し、サービス提供可否を判定するサービス提供デバイスにおいて、

前記電子鍵データは、電子鍵を識別するための主 I D データおよび副 I D データを有し、

前記サービス提供デバイスは、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、

利用者モジュールから電子鍵の一部無効化指示または全体無効化指示を受け付ける無効化受付手段と、

一部無効化指示を受け付けた場合に、前記指示に含まれる主 I D データおよび副 I D データを、前記サービス拒否情報に追加する追加手段と

全体無効化指示を受け付けた場合に、前記指示に含まれる主 I D データを、前記サービス許可情報から削除する削除手段と、を有すること

を特徴とする前記サービス提供デバイス。

#### 【請求項 1 1】

サービス提供を受けるための電子鍵データを管理する電子鍵管理装置であって、

前記電子鍵管理装置は、電子鍵を識別するための主 I D データと、電子鍵を識別するための副 I D データと、電子鍵の共有可能な範囲を示す共有階層データとを有する電子鍵データを記憶する記憶手段と、

ネットワークで接続された端末装置から入力された副 I D データを含む電子鍵の共有要求を受け付ける共有要求手段と、



共有階層データを参照して共有可能か否かを判定する共有判定手段と、  
共有可能な場合に、共有用電子鍵データを生成する生成手段と、を有すること  
を特徴とする電子鍵管理装置。

【請求項 1 2】

サービス提供を受けるための電子鍵データを管理する電子鍵管理装置であって

、  
前記電子鍵管理装置は、サービス提供を許可するためのサービス許可情報、お  
よび、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、  
外部システムから電子鍵データを受け付ける受付手段と、

前記受け付けた電子鍵データと、前記サービス許可情報と、前記サービス拒否  
情報にもとづき、前記受け付けた電子鍵データのサービス提供可否を判断する判  
断手段と、を有すること、

を特徴とする電子鍵管理装置。

【請求項 1 3】

電子鍵を利用して住宅のドアの開錠または施錠を行うドアの開錠施錠システム  
において、

電子鍵を識別するための主 I D および副 I D を有する電子鍵データを記憶した  
I C カードと、前記電子鍵データの正当性を判定しドアの開錠または施錠を行う  
デバイスとを有し、

前記 I C カードは、前記デバイスからの電子鍵の送信要求を受け付け、電子鍵  
データを前記デバイスに送信する送信手段を有し、

前記デバイスは、サービス提供を許可するためのサービス許可情報、および、  
サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、I C カ  
ードから電子鍵データを受け付ける手段と、前記受け付けた電子鍵データの主 I  
D が、前記サービス許可情報に存在するか否かを判定する第 1 の判定手段と、前  
記受け付けた電子鍵データの副 I D が、前記サービス拒否情報に存在するか否か  
を判定する第 2 の判定手段とを有し、

前記デバイスは、前記第 1 および第 2 の判定結果により、前記受け付けた電子  
鍵データの正当性を判断し、ドアの開錠または施錠を行う実行手段と、を有する

こと、

を特徴とするドアの開錠施錠システム。

**【請求項 14】**

レンタカーの鍵として電子鍵を使用し、レンタカーの鍵を利用者に提供するレンタカーサービスシステムにおいて、

電子鍵を識別するための主 I D および副 I D を有する電子鍵データを記憶した I C カードと、前記電子鍵データの正当性を判定してレンタカーの利用を許可するデバイスと、サービス提供を受けるための電子鍵データを管理する電子鍵管理装置とを有し、

前記電子鍵管理装置は、外部システムから選択されたレンタカーを、識別する主 I D および副 I D を有する電子鍵を生成する生成手段と、生成した電子鍵を利用者の I C カードに送信する送信手段と、主 I D を前記デバイスに送信する送信手段とを有し、

前記 I C カードは、前記生成された電子鍵を記憶する記憶手段を有し、

前記デバイスは、前記送信された主 I D を、提供を許可するためのサービス許可情報に記憶する記憶手段を有すること

を特徴とするレンタカーサービスシステム。

**【請求項 15】**

サービス提供可否を判断するサービス提供デバイスが、サービス提供可否を判断するための利用するコンピュータ装置の利用プログラムにおいて

前記コンピュータ装置に、電子鍵を識別するための主 I D データおよび副 I D データを記憶する記憶手段と、

前記サービス提供デバイスから電子鍵の送信要求を受け付ける送信要求受付手段と、電子鍵データを前記サービス提供デバイスに送信する送信手段とを機能させること、

を特徴とする利用プログラム。

**【請求項 16】**

請求項 15 に記載の利用プログラムにおいて、

前記コンピュータ装置に、電子鍵の共有可能か否かを示す共有階層データを記

憶する記憶手段と、

電子鍵の共有要求を受け付ける共有要求受付手段と、

共有可能な場合に、主 I D が同一で、かつ副 I D が異なる共有用電子鍵データを生成する生成手段と、

前記生成した共有用電子鍵データを、外部システムに送信する送信手段とを機能させること、

を特徴とする利用プログラム。

#### 【請求項 1 7】

利用者モジュールに記憶された電子鍵データを利用し、サービス提供可否をコンピュータ装置に判断させるサービス提供可否判断プログラムにおいて

コンピュータ装置に、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、

利用者モジュールから電子鍵データを受け付ける受付手段と、

前記受け付けた電子鍵データと、前記サービス許可情報と、前記サービス拒否情報とにものとづき、前記受け付けた電子鍵データのサービス提供可否を判断する判断手段として機能させること

を特徴とするサービス提供可否判断プログラム。

#### 【請求項 1 8】

電子鍵を利用しサービス提供を行う電子鍵利用方法において、

サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶ステップと、

外部システムから、電子鍵を識別するための主 I D データおよび副 I D データを含む電子鍵データを受け付ける受付ステップと、

前記受け付けた電子鍵データの主 I D が、前記サービス許可情報に存在するか否かを判定する第 1 の判定ステップと、

前記受け付けた電子鍵データの副 I D が、前記サービス拒否情報に存在するか否かを判定する第 2 の判定ステップと、

前記第 1 および第 2 の判定ステップの結果に応じて、前記受け付けた電子鍵データのサービス提供可否を判断する提供可否判断ステップと、を有すること

を特徴とする電子鍵利用方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ＩＣカードなどのデバイスに電子鍵を格納し、各種サービスの提供可否を判定する電子鍵システムおよび電子鍵利用方法に係わり、特に複数の利用者間で電子鍵を共有する電子鍵方法および電子鍵システムに係わる。

【0 0 0 2】

【従来の技術】

各種サービスの提供可否を判定する手段として、ＩＣカードに格納された電子鍵を利用するサービス提供方法が開示されている（特許文献１参照）。具体的には、予約したホテルの部屋、あるいは、レンタカーの鍵を電子鍵としてＩＣカードに格納し、サービス提供場所に設置されたサービス提供可否を判断する装置が、該ＩＣカードから電子鍵を読み出し、読み出した電子鍵の情報を正当と判定した場合に、ドアの開錠などを実行する。

【0 0 0 3】

また、ＩＣカードから電子鍵を読み出し、電子鍵の情報の正当性を判定してサービス提供の可否を判断する装置についても開示されている（特許文献１および特許文献２参照）。

【0 0 0 4】

【特許文献１】

特開 2 0 0 2 - 2 7 9 3 6 0 号公報

【特許文献２】

特開平 7 - 2 3 3 6 6 3 号公報

【0 0 0 5】

【発明が解決しようとする課題】

上記従来技術では、複数の利用者が電子鍵を共有してサービスを共同利用する方法について開示されていない。また、電子鍵を共有する簡単な方法としては、利用者が保有するＩＣカードに同一の電子鍵をコピーし、電子鍵を共有する方法

が考えられるが、次のような問題が生じる。例えば、同一の電子鍵をコピーした I C カードのうちのいずれかが紛失あるいは盗難した場合、紛失等された I C カードの不正利用を防止するために、当該電子鍵をサービス提供者装置において無効にする必要がある。しかし、同一の複数の電子鍵のうちのいずれか 1 つを無効にした場合は、他の残りの電子鍵の全てが無効となってしまう。

#### 【 0 0 0 6 】

本発明は上記事情を考慮してなされたものであり、本発明の目的は利用者が共有する電子鍵の一部を無効化した場合であっても、他の電子鍵を必ずしも無効とする必要がないようにすることにある。

#### 【 0 0 0 7 】

##### 【課題を解決するための手段】

上記課題を解決するために、本発明は、利用者の保有する I C カードなどの利用者モジュールに、第 1 の識別子である主 I D データと、第 2 の識別子である副 I D データから構成される電子鍵データを格納し、サービス利用可否を判定するサービス提供デバイスにおいては、サービス許可テーブルとサービス拒否テーブルの 2 つのテーブルを保持し、サービス提供デバイスは該電子鍵データの正当性を判断する。

#### 【 0 0 0 8 】

例えば、電子鍵を利用してサービス提供を行う電子鍵システムにおいて、電子鍵を識別するための主 I D および副 I D を有する電子鍵データを記憶した利用者モジュールと、サービス提供可否を判定するサービス提供デバイスとを有する。そして、前記利用者モジュールは、サービス提供デバイスからの電子鍵の送信要求を受け付ける受付手段と、電子鍵データを前記サービス提供デバイスに送信する送信手段を有し、前記サービス提供デバイスは、サービス提供を許可するためのサービス許可情報、および、サービス提供を拒否するためのサービス拒否情報を記憶する記憶手段と、利用者モジュールから電子鍵データを受け付ける受付手段と、前記受け付けた電子鍵データの主 I D が、前記サービス許可情報に存在するか否かを判定する第 1 の判定手段と、前記受け付けた電子鍵データの副 I D が、前記サービス拒否情報に存在するか否かを判定する第 2 の判定手段とを有し、

前記サービス提供デバイスは、前記第 1 および第 2 の判定結果により、サービス提供可否を判断する提供判断手段と有する電子鍵システムを提供する。

#### 【0 0 0 9】

#### 【発明の実施の形態】

以下に、本発明に係る第 1 の実施の形態について説明する。本実施の形態は、住宅のドアの鍵に電子鍵を適用した場合の実施形態である。

#### 【0 0 1 0】

図 1 に、本発明を適用した電子鍵システムのシステム構成図を示す。

#### 【0 0 1 1】

図示するように、本実施形態のシステムは、利用者モジュール 1 0 0、利用者端末 2 0 0、電子鍵管理装置 3 0 0 およびサービス提供デバイス 4 0 0 を有する。これらは、インターネットなどのネットワーク 5 2 0 により相互に接続される。

#### 【0 0 1 2】

利用者モジュール 1 0 0 は、電子鍵データを格納し、後述する所定の処理に応じて電子鍵データの送信、生成などを行うデバイスである。電子鍵の偽造、不正コピーなどを防止するために、利用者モジュール 1 0 0 は、I C カードなど耐タンパ性を有するデバイスを用いることが望ましい。

#### 【0 0 1 3】

利用者端末 2 0 0 は、サービスの利用を希望する利用者が保有する端末である。携帯タイプの端末 2 0 0 は携帯電話網などのネットワーク 5 1 0 を介してネットワーク 5 2 0 に接続される。

#### 【0 0 1 4】

電子鍵管理装置 3 0 0 は、利用者からの要求に応じて電子鍵を発行、無効化するなどの電子鍵の各種管理を行う。例えば、WEB サイトなどである。サービス提供デバイス 4 0 0 は、利用者モジュール 1 0 0 に格納されている電子鍵の正当性を判定し、その結果に応じてサービス提供可否を判定するデバイスである。本実施形態において、サービス提供デバイス 4 0 0 は、利用者の住宅のドアに取り付けられ、電磁式ロックなどと接続して電子鍵の正当性を判定し、正当な電子鍵

の場合にドアを開錠または施錠を実行するデバイスである。

【 0 0 1 5 】

次に、電子鍵システムのハードウェア構成について説明する。

【 0 0 1 6 】

図 2 は、図 2 に示すように、利用者モジュール 1 0 0、利用者端末 2 0 0、電子鍵管理装置 3 0 0、サービス提供デバイス 4 0 0 の各装置のハードウェア構成を示したものである。

【 0 0 1 7 】

利用者端末 2 0 0 は、例えば、プログラムに従ってデータの加工・演算を行なう CPU 9 0 1 と、CPU 9 0 1 が直接読み書き可能なメモリ 9 0 2 と、ハードディスク等の外部記憶装置 9 0 3 と、外部システムとデータ通信をするために通信装置 9 0 4 と、キーボード、キーボタン、音声入力装置等の入力装置 9 0 5 と、ディスプレイまたはプリンタ等の出力装置 9 0 6 とを有する一般的なコンピュータシステムを利用することができる。具体的には、携帯電話、利用者簡易携帯電話 (PHS: Personal Handy-Phone System)、PDA (Personal Digital Assistant)、PC (Personal Computer) などである。

【 0 0 1 8 】

電子鍵管理装置 3 0 0 は、前記利用者端末 2 0 0 と同様の一般的なコンピュータシステムを利用することができる。具体的には、サーバ、ホストコンピュータなどである。

【 0 0 1 9 】

利用者モジュール 1 0 0 は、図 2 に示す構成のうち、少なくとも、プログラムに従ってデータの加工・演算を行なう CPU 9 0 1 と、CPU 9 0 1 が直接読み書き可能なメモリ 9 0 2 と、外部システムとデータ通信をするために通信装置 9 0 4 とを有するコンピュータ装置であり、例えば IC カードなどを利用することができる。

【 0 0 2 0 】

サービス提供デバイス 4 0 0 は、図 2 に示す構成のうち、少なくとも、プログラムに従ってデータの加工・演算を行なう CPU 9 0 1 と、CPU 9 0 1 が直接

読み書き可能なメモリ 9 0 2 と、外部システムとデータ通信をするために通信装置 9 0 4 とを有するコンピュータ装置である。

#### 【 0 0 2 1 】

次に、電子鍵システムの機能構成について説明する。

#### 【 0 0 2 2 】

図 3 は、図 1 に示す各装置の機能構成を示した図である。以下に述べる各装置の各機能は、各メモリ 9 0 2 にロードまたは記憶された所定のプログラムを、利用者モジュール 1 0 0 プログラムの場合は利用者モジュール 1 0 0 の CPU 9 0 1 が、利用者端末 2 0 0 用のプログラムの場合は利用者端末 2 0 0 の CPU 9 0 1 が、電子鍵管理装置 3 0 0 用のプログラムの場合は電子鍵管理装置 3 0 0 の CPU が、サービス提供デバイス 4 0 0 用のプログラムの場合はサービス提供デバイス 4 0 0 の CPU 9 0 1 が、それぞれ実行することにより、実現される。

#### 【 0 0 2 3 】

利用者モジュール 1 0 0 は、制御部 1 8 1、記憶部 1 8 2、利用者端末通信部（以下、「UT 通信部」） 1 8 3、および近距離無線通信部 1 8 4 を有する。制御部 1 8 1 は、利用者モジュール 1 0 0 内の各部の制御を行う。記憶部 1 8 2 は、プログラムおよびデータをメモリ 9 0 2 に記憶する。UT 通信部 1 8 3 は、通信装置 9 0 4 により、利用者端末 2 0 0 とデータの送受信を行う。そして、近距離無線通信部 1 8 4 は、通信装置 9 0 4 により、サービス提供デバイス 4 0 0 または他の利用者モジュール 1 0 0 と、無線通信によりデータ送受信を行う。このような無線通信の例としては、無線 LAN、ISO/IEC14443 などがある。なお、利用者端末 2 0 0 が近距離無線通信部 1 8 4 を有し、利用者モジュール 1 0 0 は利用者端末 2 0 0 を介してサービス提供デバイス 4 0 0 などと通信する構成としても良い。

#### 【 0 0 2 4 】

利用者端末 2 0 0 は、制御部 2 8 1、記憶部 2 8 2、入力部 2 8 3、遠距離無線通信部 2 8 4、表示部 2 8 5 および利用者モジュール通信部（以下、「UM 通信部」） 2 8 6 を有する。制御部 2 8 1 は、利用者端末 2 0 0 内の各部の制御を行う。記憶部 2 8 2 は、プログラムおよびデータを外部記憶装置 9 0 3 に記憶す



る。入力部 2 8 3 は、入力装置 9 0 5 により、利用者からのデータ入力を受け付ける。遠距離無線通信部 2 8 4 は、通信装置 9 0 4 により、電子鍵管理装置 3 0 0 または他の利用者端末 2 0 0 とデータの送受信を行う。表示部 2 8 5 は、出力装置 9 0 6 により、利用者へデータの表示を行う。そして、UM通信部 2 8 6 は、利用者モジュール 1 0 0 とのデータ送受信を行う。

#### 【 0 0 2 5 】

電子鍵管理装置 3 0 0 は、制御部 3 8 1、記憶部 3 8 2 および通信部 3 8 3 を有する。制御部 3 8 1 は、電子鍵管理装置 3 0 0 内の各部の制御を行う。記憶部 3 8 2 は、プログラムおよびデータを外部記憶装置 9 0 3 に記憶する。通信部 3 8 3 は、ネットワーク 5 2 0 を介して、通信装置 9 0 4 により、利用者端末 1 0 0 またはサービス提供デバイス 2 0 0 とデータの送受信を行う。

#### 【 0 0 2 6 】

サービス提供デバイス 4 0 0 は、制御部 4 8 1、記憶部 4 8 2 および通信部 4 8 3、近距離無線通信部 2 4 8 を有する。制御部 4 8 1 は、サービス提供デバイス 4 0 0 内の各部の制御を行う。記憶部 4 8 2 は、プログラムおよびデータをメモリ 9 0 2 に記憶する。通信部 4 8 3 は、通信装置 9 0 4 により、電子鍵管理装置 3 0 0 とデータの送受信を行う。近距離無線通信部 2 4 8 は、利用者モジュール 1 0 0 とデータ送受信を行う。

#### 【 0 0 2 7 】

次に、電子鍵システムに用いられる各種のデータのデータ構成図について説明する。

#### 【 0 0 2 8 】

図 4 は、電子鍵システムに用いられる各種のデータのデータ構成図を示したものである。図示するように、利用者モジュール 1 0 0、電子鍵管理装置 3 0 0、サービス提供デバイス 4 0 0 に以下に説明する各種のデータが格納されている。

#### 【 0 0 2 9 】

利用者モジュール 1 0 0 には、暗号鍵である利用者モジュール認証鍵データ（以下、「UM認証鍵データ」） 1 1 0 と、利用者電子鍵テーブル 1 2 0 が格納されている。UM認証鍵データ 1 1 0 は、後述する相互認証処理において使用され

る暗号鍵データである。暗号鍵データには、例えば共通鍵暗号系における共通鍵を用いることが考えられる。共通鍵暗号系の例としては、DES(Data Encryption Standard)、AES(Advanced Encryption Standard)などがあげられる。

#### 【0 0 3 0】

利用者電子鍵テーブル 1 2 0 は、利用者が保有する電子鍵の情報が格納されたデータの集合である。利用者電子鍵テーブル 1 2 0 は、電子鍵の名前を表す鍵名称、電子鍵を識別するための第 1 の識別子である主 I D、電子鍵の共有可能な範囲を示す共有階層、電子鍵を識別するための第 2 の識別子である副 I D の履歴とを有する。

#### 【0 0 3 1】

鍵名称には、電子鍵の対象となるサービス提供デバイス 4 0 0 を、利用者が識別するための名称（例えば「X X 宅」など）を設定する。主 I D には、発行済みの他の電子鍵と識別するために、他の電子鍵の主 I D とは異なる一意性（ユニーク）のある I D を設定する。例えば、電子鍵管理装置 3 0 0 において、シリアル番号を管理し、電子鍵の発行ごとにその値をカウントアップして、順次カウントアップされた値を設定することが考えられる。

#### 【0 0 3 2】

共有階層には、「0」または「1」以上の数値が設定される。「0」の場合は、電子鍵の共有が不可能なことを意味する。また、例えば共有階層に「2」が設定されている場合は、その電子鍵は第 1 の共有階層として利用者 A から利用者 B に共有が許可され、更に第 2 の共有階層として利用者 B から利用者 C に共有が許可される。また共有階層に「1」が設定されている場合は、第 1 の共有階層として利用者 A から利用者 B への共有は許可されるが、更に第 2 の共有階層として利用者 B から利用者 C への共有は禁止される。なお、電子鍵の共有が不可能なことを意味する値は「0」に限られず、あらかじめ定めた所定の値であればよい。

#### 【0 0 3 3】

副 I D は、電子鍵を識別するための第 2 の識別子であり、副 I D 履歴には複数の副 I D データを格納できる。電子鍵管理装置 3 0 0 が利用者に新たな利用者モジュールを発行または提供する際に、副 I D 履歴には、後述する顧客テーブル 3

3 0 の副 I D に設定されているデータが設定される。本実施の形態においては、副 I D として、利用者の携帯番号を使用している。

#### 【 0 0 3 4 】

電子鍵管理装置 3 0 0 には、サービスデバイス認証鍵データ（以下、「S D 認証鍵データ」） 3 1 0、U M 認証鍵データ 3 2 0 および顧客テーブル 3 3 0 が格納されている。S D 認証鍵データ 3 1 0 および U M 認証鍵データ 3 2 0 は、U M 認証鍵データ 1 1 0 と同様に相互認証処理で使用される暗号鍵データである。共通鍵暗号系を用いる場合、電子鍵管理装置 3 0 0 の U M 認証鍵データ 3 2 0 は、利用者モジュール 1 0 0 の U M 認証鍵データ 1 1 0 と同値のデータが設定される。

#### 【 0 0 3 5 】

顧客テーブル 3 3 0 は、利用者に関する各種の情報を管理するデータの集合である。顧客テーブル 3 3 0 は、利用者を一意に識別する会員番号、利用者を認証するための英数字列などから構成されるパスワード、電子鍵を共有する場合に共有者内で利用者を識別するための副 I D、その利用者に割り当てられた電子鍵を識別するための主 I D、S D アドレスを有する。主 I D には、サービスの利用を申し込んだ利用者の利用者モジュール 1 0 0 に設定された主 I D と同一の値を設定する。副 I D は、前述の利用者電子鍵テーブル 1 2 0 の副 I D に最初に設定された副 I D データと同一の値を設定する。なお、サービス本実施の形態において、副 I D は携帯電話番号を用いている。S D アドレスは、ネットワーク 5 2 0 におけるサービス提供デバイス 4 0 0 のネットワークアドレスであり、電子鍵管理装置 3 0 0 がサービス提供デバイス 4 0 0 に対して、データの送受信を行うために使用される。具体的には、I P アドレスなどが適用される。

#### 【 0 0 3 6 】

サービス提供デバイス 4 0 0 には、S D 認証鍵データ 4 1 0、U M 認証鍵データ 4 2 0、サービス許可テーブル 4 3 0 およびサービス拒否テーブル 4 4 0 が格納されている。S D 認証鍵データ 4 1 0 および U M 認証鍵データ 4 2 0 は、U M 認証鍵データ 1 1 0 等と同様に相互認証処理で使用される暗号鍵データである。共通鍵暗号系を用いる場合、サービス提供デバイス 4 0 0 の S D 認証鍵データ 4

1 0 は、電子鍵管理装置 3 0 0 の S D 認証鍵データ 3 1 0 と、同値のデータが設定される。また、サービス提供デバイス 4 0 0 の U M 認証鍵データ 4 2 0 は、電子鍵管理装置 3 0 0 の U M 認証鍵データ 3 2 0 および利用者モジュール 1 0 0 の U M 認証鍵データ 1 1 0 と同値のデータが設定される。

#### 【 0 0 3 7 】

サービス許可テーブル 4 3 0 は、サービス提供デバイス 4 0 0 において、サービスの利用が許可される電子鍵を識別するためのテーブルであり、サービスの利用が許可される主 I D のデータを有する。サービス拒否テーブル 4 4 0 は、サービス提供デバイス 4 0 0 において、サービスの利用が禁止される電子鍵を識別するためのテーブルであり、サービスの利用が禁止される主 I D および副 I D のデータを有する。なお、サービス許可テーブル 4 3 0 およびサービス拒否テーブル 4 4 0 の主 I D には、当該サービス提供デバイス 4 0 0 を利用する利用者モジュールに設定された主 I D と同一の値が設定される。

#### 【 0 0 3 8 】

なお、本実施形態においては、図 4 に示した各種のデータは、サービス拒否テーブル 4 4 0 のデータを除き、各装置のメモリ 9 0 2 または外部記憶装置 9 0 3 にあらかじめ設定されているものとする。例えば、利用者がサービス提供者にサービスの利用を申し込んだタイミングで、電子鍵管理装置 3 0 0 は各装置のメモリ 9 0 2 または外部記憶装置 9 0 3 に所定のデータを設定し、利用者モジュール 1 0 0、サービス提供デバイス 4 0 0 などの配布および設置を行う。

#### 【 0 0 3 9 】

次に、図 5 を参照し、本実施形態において利用者がサービス提供（住宅のドアを開錠する）を受けるときの処理の流れを説明する。

#### 【 0 0 4 0 】

サービス提供デバイス 4 0 0 の近距離無線通信部 4 8 4 は、電子鍵送信要求メッセージを利用者モジュール 1 0 0 に定期的に送信する（ステップ 1 0 1）。利用者モジュール 1 0 0 の近距離無線通信部 1 8 4 が、該メッセージを受信すると、制御部 1 8 1 は、サービス提供デバイス 4 0 0 の制御部 4 8 1 との間で相互認証処理を実行する（ステップ 1 0 2）。該相互認証処理は、例えば、利用者モジ

ユーモール 1 0 0 とサービス提供デバイス 4 0 0 の各々の U M 認証鍵データ 1 1 0、4 2 0 を使用し、共通鍵を利用した相互認証手順の規定である ISO/IEC 9798-2 に記載の「5.2.2 Three pass authentication」に従って実行される。このような相互認証処理を実行することにより、悪意の第 3 者が偽の利用者モジュール 1 0 0 を利用してサービス提供を受けることを防止する。また、偽のサービス提供デバイス 4 0 0 に対して、利用者モジュール 1 0 0 が電子鍵を誤って送信し、その結果として電子鍵の内容が露呈することを防止する。

#### 【 0 0 4 1 】

また、該相互認証が終了した後は、セッション鍵などにより、以降の送信メッセージ内容を暗号化することが望ましい。該セッション鍵としては、前記「Three pass authentication」の処理中に生成される乱数を使用する方法がある。このようなメッセージの暗号化を行うことにより、メッセージ盗聴による電子鍵の露呈を防止することが可能である。

#### 【 0 0 4 2 】

次に、利用者モジュール 1 0 0 の近距離無線通信部 1 8 4 は、サービス提供デバイス 4 0 0 に電子鍵送信メッセージを送信する（ステップ 1 0 3）。該メッセージは、利用者電子鍵テーブル 1 2 0 に保持されるデータのうち、少なくとも主 I D データと副 I D 履歴データを含むものとする。

#### 【 0 0 4 3 】

サービス提供デバイス 4 0 0 の近距離無線通信部 4 8 4 は、該メッセージを受信し、次に、制御部 4 8 1 が受信した主 I D データが、サービス許可テーブル 4 3 0 内に存在するか否かを判定する（ステップ 1 0 4）。主 I D データが存在する場合（ステップ 1 0 4 で Y E S）は、制御部 4 8 1 は、受信した副 I D 履歴データに含まれる副 I D データが、サービス拒否テーブル 4 4 0 に存在するか否かを判定する（ステップ 1 0 5）。制御部 4 8 1 は、この判定において、受信した副 I D 履歴データに含まれる副 I D データのうち、一つでもサービス拒否テーブル 4 4 0 に存在する場合は、「存在する」と判定する。したがって、サービス拒否テーブル 4 4 0 に存在する副 I D データを副 I D 履歴に有する利用者鍵テーブルの利用者モジュールは、サービス提供が拒否される。このことにより、該副 I

Dから共有を許可された利用者モジュール（該副IDより下位の共有先の利用者モジュール）の使用ができなくなり、紛失または盗難された利用者モジュールから電子鍵をコピーするなど、悪用されることを防止することが可能となる。

#### 【0044】

副IDが存在しないと判定した場合（ステップ105でNO）は、制御部481はサービス提供を許可する処理を実行する（ステップ106）。本実施形態においては、住居のドアの開錠処理を実行する。

#### 【0045】

また、副IDが存在すると判定した場合（ステップ105でYES）は、制御部481はサービス提供を拒否し処理を終了する（ステップ107）。本実施形態においては、住居のドアの開錠処理を実行せずに施錠したままとする。また、主IDがサービス許可テーブルに存在しない場合（ステップ104でNO）の場合も、制御部481はサービス提供を拒否し処理を終了する（ステップ107）。

#### 【0046】

上記の処理は、利用者モジュール100が電子鍵を近距離無線通信184により送信する方式について説明したが、他の方式により送信しても良い。例えば、ネットワーク510およびネットワーク520を経由して送信するようにしても良い。この場合の処理の流れを以下に説明する。本処理は、図5の処理を比較すると、電子鍵送受信処理（ステップ101からステップ103）の部分においてのみ異なり、他の部分は図5の処理と同じであるため、相違する部分について図6を参照し説明する。

#### 【0047】

図6は、利用者端末200を利用して、利用者がサービス提供を受けるときの電子鍵送受信処理の流れを示したものである。

#### 【0048】

利用者端末200の入力部283が、利用者の操作指示を受け付けると、UM部286は電子鍵送信要求メッセージを利用者モジュール100に送信する（ステップ201）。利用者モジュール100のUT通信部138が、該メッセージ

を受信すると、制御部 1 8 1 は、サービス提供デバイス 4 0 0 の制御部 4 8 1 との間で相互認証処理を実行する（ステップ 2 0 2）。該相互認証処理は、利用者端末 2 0 0、ネットワーク 5 1 0 およびネットワーク 5 2 0 を介して実行する。該相互認証処理において使用する認証鍵データ、相互認証手順、その後のメッセージの暗号化などについては、図 5 のステップ 1 0 2 の処理と同様である。

#### 【 0 0 4 9 】

次に、利用者モジュール 1 0 0 の UT 通信部 1 3 8 は、サービス提供デバイス 4 0 0 に電子鍵送信メッセージを送信する（ステップ 2 0 3）。該メッセージ送信において、利用者端末 2 0 0、ネットワーク 5 1 0などを介する点は、ステップ 2 0 2 と同様である。ステップ 2 0 3 の処理の後には、図 5 に記載されているステップ 1 0 4 以降の処理を、サービス提供デバイス 4 0 0 が実行する。

#### 【 0 0 5 0 】

このような各種ネットワークを介した電子鍵の送信を行うことにより、例えば、電子鍵である利用者モジュール 1 0 0 を保有する利用者が、外出して自宅にいないときに、知人が自宅を訪問した場合、利用者端末 2 0 0 から遠隔で自宅のドアの開錠を実行して知人に自宅で待ってもらう、というケースに対応できる。

#### 【 0 0 5 1 】

次に、サービス利用者の中で、電子鍵を共有する場合の処理について説明する。図 7 は、電子鍵の共有処理の流れを示し、図 1 1 は、共有処理において利用者端末 2 0 0 に表示される表示画面の例を示したものである。本処理においては、電子鍵の共有元となる利用者が保有する利用者モジュール 1 0 0 および利用者端末 2 0 0 を、第 1 の利用者モジュール 1 0 0 および第 1 の利用者端末 2 0 0 とする。また、電子鍵の共有先の利用者が保有する利用者モジュール 1 0 0 および利用者端末 2 0 0 を、第 2 の利用者モジュール 1 0 0 および第 2 の利用者端末 2 0 0 とする。また、図 1 1 の表示画面の例では、副 ID に携帯電話番号を使用している。

#### 【 0 0 5 2 】

まず初めに、第 1 の利用者端末 2 0 0 の入力部 2 8 3 が、共有元の利用者の操作指示を受け付けると、UM 通信部 2 8 4 が電子鍵一覧要求メッセージを第 1 の

利用者モジュール 1 0 0 に送信する（ステップ 3 0 1）。第 1 の利用者モジュール 1 0 0 の U T 通信部 1 8 3 は該メッセージを受信し、次に制御部 1 8 1 が利用者電子鍵テーブル 1 2 0 に格納されている各レコードの鍵名称データおよび主 I D データのペアを、格納レコードの数だけ電子鍵一覧応答メッセージに設定する。そして U T 通信部 1 8 3 は、第 1 の利用者端末 2 0 0 に電子鍵一覧応答メッセージを送信する（ステップ 3 0 2）。

#### 【 0 0 5 3 】

第 1 の利用者端末 2 0 0 の U M 通信部 2 8 4 は該メッセージを受信し、表示部 2 8 5 が受信した鍵名称データの一覧を出力装置 9 0 6 に表示する（画面 3 1）。そして、第 1 の利用者端末 2 0 0 の入力装置 9 0 5 は、利用者が選択データの一覧から選択した鍵名称の選択指示を受け付ける（ステップ 3 0 3）。

#### 【 0 0 5 4 】

次に、第 1 の利用者端末 2 0 0 の表示部 2 8 5 は、副 I D データ入力画面を出力装置 9 0 6 に表示する（画面 3 2）。そして入力装置 9 0 5 は、利用者の入力した副 I D データを受け付ける。副 I D データは、利用者モジュール 1 0 0 が紛失あるいは盗難された場合に、該利用者モジュール 1 0 0 の電子鍵のみを無効化するために必要なデータであり、電子鍵を共有する利用者のグループの中で一意となるデータを用いるものとする。本実施形態においては、利用者の電話番号を副 I D として使用する。そして U M 通信部 2 8 4 は、共有開始メッセージを第 1 の利用者モジュール 1 0 0 に送信する（ステップ 3 0 4）。該メッセージは、ステップ 3 0 3 で選択された主 I D データと、ステップ 3 0 4 で入力された副 I D データを含む。該メッセージを送信した後、第 1 の利用者端末 2 0 0 の表示部 2 8 5 は、「コピー処理中」の画面を出力装置 9 0 6 に表示する（画面 3 3）。

#### 【 0 0 5 5 】

第 1 の利用者モジュール 1 0 0 の U T 通信部 1 8 3 は該メッセージを受信し、制御部 1 8 1 が共有先の第 2 の利用者モジュール 1 0 0 に送信する利用者電子鍵テーブル 1 2 0 のデータを生成する（ステップ 3 0 5）。利用者電子鍵テーブル 1 2 0 は、図 4 で説明したデータの集合である。主 I D には共有開始メッセージに含まれる主 I D データを設定し、鍵名称には該主 I D データから特定されるレ



コードの鍵名称を設定する。共有階層には、該レコードの共有階層の値から 1 を引いた値を設定する。ただし、引いた後の値がマイナスの数値となる場合は、これ以上の電子鍵の共有は許可されていないと判定し、以降の処理を実行せずに処理を終了する。副 ID 履歴データには、共有開始メッセージに含まれる副 ID データを追加して設定する。

#### 【0056】

次に、第 1 の利用者モジュール 100 と、第 2 の利用者モジュール 100 は、相互認証処理を実行する（ステップ 306）。この相互認証処理で使用する認証鍵としては、各々の利用者モジュールが保持する UM 認証鍵データ 110 を使用する。また、該相互認証処理は各々の利用者端末 200 およびネットワーク 510 を介して行われる。なお、該相互認証処理は、各々の近距離無線通信部 184 を介し、第 1 の利用者モジュール 100 と第 2 の利用者モジュール 100 との間で直接行うこととしても良い。その他の該相互認証処理については、図 5 のステップ 102 と同様であり、また、以降のメッセージ暗号化についても同様である。

#### 【0057】

次に、第 1 の利用者モジュール 100 は、電子鍵書込メッセージを第 2 の利用者モジュール 100 に送信する（ステップ 307）。このとき、該メッセージの送信経路についてはステップ 306 の場合と同様である。該メッセージは、ステップ 305 で生成した利用者電子鍵テーブル 120 のデータを含む。第 2 の利用者モジュール 200 は、電子鍵書込メッセージを受信し、該メッセージ中の利用者電子鍵テーブル 120 のデータ（レコード）を、既存の利用者電子鍵テーブル 120 に追加する（ステップ 308）。本処理が終了した後、第 1 の利用者端末 200 の表示部 285 は、「コピー終了」の画面を出力装置 906 に表示する（画面 34）。以上により、電子鍵の共有処理を終了する。

#### 【0058】

次に、電子鍵の共有処理における利用者電子鍵テーブル 120 について説明する。図 8 は、第 1 の利用者モジュール 100 の利用者電子鍵テーブル 121（以下、「第 1 の利用者電子鍵テーブル」）に設定された共有階層の値が「1」のと

きの第1の利用者モジュール100と、第2の利用者モジュール100の利用者電子鍵テーブル122（以下、「第2の利用者電子鍵テーブル」）を示したものである。

#### 【0059】

第1の利用者電子鍵テーブル121は、電子鍵の共有処理の前後において、データの変更はない。第2の利用者電子鍵テーブル122には、鍵名称、主IDが第1の利用者電子鍵テーブル121と同じ値が設定され、共有階層に第1の利用者電子鍵テーブル121の値から「1」を引いた値「0」が設定され、副履歴IDには第1の利用者端末200から入力された携帯番号が設定されたレコードが新規に追加される。この場合、第2の利用者鍵テーブルの共有階層は「0」であるため、第2の利用者は電子鍵の共有処理を行うことはできない。

#### 【0060】

図9は、共有元である第1の利用者電子鍵テーブル121の共有階層が「3」のときの、第1の利用者電子鍵テーブル121、第2の利用者電子鍵テーブル122、第3の利用者電子鍵テーブル123（第3の利用者モジュール100の利用者電子鍵テーブル）、第4の利用者電子鍵テーブル124（第4の利用者モジュール100の利用者電子鍵テーブル）示したものである。

#### 【0061】

第2の利用者電子鍵テーブル122には、共有階層に第1の利用者電子鍵テーブル121の値から「1」を引いた値「2」が設定され、その他は図8と同様のレコードが新規に追加される。次に、第3の利用者電子鍵テーブル123には、共有階層が第2の利用者電子鍵テーブル122の値から「1」を引いた値「1」が設定され、副履歴IDには第2の利用者電子鍵テーブル122に設定された携帯番号と第2の利用者端末200から入力された携帯番号とが設定されたレコードが新規に追加される。次に第3の利用者電子鍵テーブル124には、同様に、共有階層に「0」が、副履歴IDには3つの携帯番号が設定されたレコードが新規に追加される。この場合、第4の利用者鍵テーブルの共有階層は「0」であるため、第4の利用者は電子鍵の共有処理を行うことはできない。

#### 【0062】

次に、図 1 0 および図 1 1 を参照し、電子鍵を無効化するときの処理の流れを説明する。電子鍵を無効化する場合としては、利用者モジュール 1 0 0 の紛失または盗難などがあげられる。なお、ステップ 4 0 1 からステップ 4 0 5 については、既存の W E B ブラウザおよび W E B サーバなどで実現可能な処理であるため、詳細な説明は省略する。また、図 1 1 の表示画面の例では、副 I D に携帯電話番号を使用している。

#### 【 0 0 6 3 】

まず初めに、利用者端末 2 0 0 の表示部 2 8 5 が、利用者の操作指示に応じ、会員番号およびパスワードの入力を受け付ける画面を表示し（画面 4 1）、利用者から会員番号およびパスワードの入力を受け付け、遠距離無線通信部 2 8 4 がログイン要求メッセージを電子鍵管理装置 3 0 0 に送信する（ステップ 4 0 1）。ログイン要求メッセージには、利用者から入力された会員番号およびパスワードのデータを含む。電子鍵管理装置 3 0 0 の通信部 3 8 3 が該メッセージを受信すると、制御部 3 8 1 は顧客テーブル 3 3 0 を検索し、該当会員番号が存在し、かつパスワードが一致するか否かを判定する。会員番号が存在し、パスワードが一致する場合は、通信部 3 8 3 は、サービスのメニュー表示メッセージを利用者端末 2 0 0 に送信する（ステップ 4 0 2）。会員番号が存在しなかった場合、あるいはパスワードが不一致だった場合は、制御部 3 8 1 は以降の処理を行わず処理を終了する。なお、該メニュー表示メッセージは、メニュー画面を利用者端末 2 0 0 の出力装置 9 0 6 に表示させるための、コマンド識別子あるいはページ記述言語を含む。このようなページ記述言語としては、例えば H T M L（Hyper Text Markup Language）がある。

#### 【 0 0 6 4 】

利用者端末 2 0 0 の遠距離無線通信部 2 8 4 は、メニュー表示メッセージを受信し、表示部 2 8 5 は出力装置 9 0 6 にメニュー選択画面（画面 4 2）を表示する。そして、入力部 2 8 3 が、入力手段 9 0 5 により入力された利用者のメニュー選択を受け付け、その結果を遠距離無線通信部 2 8 4 が選択メニューメッセージとして電子鍵管理装置 3 0 0 に送信する（ステップ 4 0 3）。電子鍵管理装置 3 0 0 の通信部 3 8 3 が該メッセージを受信し、制御部 3 8 1 は該メッセージが

登録無効（無効化処理）のメニューを選択していると判定した場合は、副 I D 入力要求メッセージを利用者端末 2 0 0 に送信する（ステップ 4 0 4）。なお、本実施形態においては、無効化処理以外のサービスメニューは無いものとする。

#### 【 0 0 6 5 】

利用者端末 2 0 0 の遠距離無線通信部 2 8 4 は、副 I D 入力要求メッセージを受信し、表示部 2 8 5 は出力装置 9 0 6 に副 I D 入力受付画面（画面 4 3）を表示する。そして、入力部 2 8 3 が、入力手段 9 0 5 により入力された副 I D データを受け付け、遠距離無線通信部 2 8 4 が副 I D 登録メッセージを電子鍵管理装置 3 0 0 に送信する（ステップ 4 0 5）。該メッセージには入力された副 I D データを含む。なお、該メッセージ送信後、利用者端末 2 0 0 の出力装置 9 0 6 には、「無効化登録中」画面（画面 4 4）が表示される。

#### 【 0 0 6 6 】

電子鍵管理装置 3 0 0 の通信部 3 8 3 が副 I D 登録メッセージを受信した後、制御部 3 8 1 はサービス提供デバイス 4 0 0 との間で相互認証処理を実行する（ステップ 4 0 6）。このとき、認証鍵としては電子鍵管理装置 3 0 0 とサービス提供デバイス 4 0 0 の各々の S D 認証鍵データ 3 1 0、4 1 0 を使用する。また、通信対象となるサービス提供デバイス 4 0 0 のネットワークアドレスは、ログインされた会員番号データから特定される、顧客テーブル 3 3 0 の S D アドレスデータとする。その他については、図 5 のステップ 1 0 2 の相互認証処理と同様である。

#### 【 0 0 6 7 】

次に、電子鍵管理装置 3 0 0 の制御部 3 8 1 は、ログイン処理（ステップ 4 0 2）で受信した会員番号データをキーとして顧客テーブル 3 3 0 を検索し、該当会員番号の副 I D（携帯電話番号）データを取得する。そして、制御部 3 8 1 は、利用者端末 2 0 0 から受信した副 I D 登録メッセージに含まれる副 I D データと、前記電話番号が一致するか否かを判定する（ステップ 4 0 7）。受信した副 I D データが、顧客テーブルの副 I D データと一致する場合は、共有元となる利用者モジュールが紛失または盗難等による無効化であるため、該利用モジュールの主 I D を有する電子鍵の全てを無効化する全体無効化処理を行う。一方、受信

した副 I D データが、顧客テーブルの副 I D データと一致しない場合は、利用元以外の利用者モジュール（すなわち利用先の利用者モジュール）であるため、当該副 I D を有する利用モジュールのみを無効化する部分無効化処理を行う。この部分無効化処理により、当該副 I D を有する利用モジュールから電子鍵の共有を許可された利用モジュールも無効化され、紛失等された利用モジュールの悪用を防止することができる。

#### 【 0 0 6 8 】

部分無効化処理としては、電子鍵管理装置 3 0 0 の通信部 3 8 3 は、サービス提供デバイス 4 0 0 に追加要求メッセージを送信する（ステップ 4 0 8）。該メッセージは、該当会員番号のレコードの主 I D データと、受信した副 I D 登録メッセージ内の副 I D データを含む。サービス提供デバイス 4 0 0 の通信部 4 8 3 は該追加要求メッセージを受信し、制御部 4 8 1 が、主 I D データと副 I D データを一つのレコードとしてサービス拒否テーブル 4 4 0 に追加する（ステップ 4 0 9）。なお、部分無効化処理（ステップ 4 0 9）を実行した場合は、次に述べる全体無効化処理（ステップ 4 1 0）を実行せずに、無効化終了通知（ステップ 4 1 2）を実行する。

#### 【 0 0 6 9 】

全体無効化処理として、電子鍵管理装置 3 0 0 の通信部 3 8 3 は、サービス提供デバイス 4 0 0 に削除要求メッセージを送信する（ステップ 4 1 0）。該メッセージは、該当会員番号のレコードの主 I D データを含む。サービス提供デバイス 4 0 0 の通信部 4 8 3 は該削除要求メッセージを受信し、制御部 4 8 1 が、サービス許可テーブル 4 3 0 から該当する主 I D データを削除する（ステップ 4 1 1）。

#### 【 0 0 7 0 】

部分無効化処理または全体無効化処理を終了した後、電子鍵管理装置 3 0 0 の通信部 3 8 3 は、利用者端末 2 0 0 に無効化終了通知メッセージを送信する（ステップ 4 1 2）。利用者端末 2 0 0 の遠距離無線通信部 2 8 4 は、該メッセージを受信し、表示部 2 8 5 は出力装置 9 0 6 に「無効化終了」画面（画面 4 5）を表示する。

**【0071】**

以上により、電子鍵を無効化するときの処理を終了する。

**【0072】**

なお、本実施形態において、サービス提供デバイス400に格納する副IDデータ、あるいはサービス提供デバイス400に送信されるメッセージに含まれる副IDデータは、暗号化あるいは一方向関数でダイジェスト化するようにしても良い。このような構成にした場合、サービス提供デバイス400が盗難され、その内部を解析されることにより副IDデータが露呈する（例えば電話番号を副IDデータとして利用していた場合、電話番号が露呈する）ことを防止できる。なお、一方向関数の例としては、SHA-1(Secure Hash Algorithm 1)、MD5(Message Digest 5)などがある。暗号化手段の例としては、DES(Data Encryption Standard)、AES(Advanced Encryption Standard)などの共通鍵暗号系や、楕円曲線暗号などの公開鍵暗号系がある。

**【0073】**

また、本実施形態において、副IDデータは利用者端末200から利用者が入力するようにしていたが、あらかじめ共有元の利用者の利用者端末200あるいは利用者モジュール100に格納しておいても良い。この場合、電子鍵共有処理（図7参照）の共有鍵生成処理（ステップ305）においては、利用者端末200からの副IDの入力は不要となり、このあらかじめ格納しておいた副IDデータを、共有用電子鍵データの生成に使用する。あるいは、共有先の利用者の利用者端末200または利用者モジュール100に、副IDデータを格納しておいても良い。この場合、電子鍵共有処理（図7参照）の共有鍵生成処理（ステップ305）においては、副ID履歴データに新たに副IDデータを生成せず、電子鍵書込処理（ステップ308）において、該格納済み副IDデータを利用者電子鍵テーブル120の副ID履歴に追加する。

**【0074】**

次に、本発明に係る第2の実施の形態について説明する。

**【0075】**

本実施形態は、レンタカーのドアに電子鍵を適用した場合の形態である。なお

、第 1 の実施形態と同様な点も多いので、以下に述べる説明は相違点を中心として行う。

#### 【0 0 7 6】

本実施形態のシステム構成は、第 1 の実施形態の場合とほぼ同様である（図 1 参照）。ただし、本実施形態においてサービス提供デバイス 4 0 0 は、レンタカーのドアに取り付けられ、電子鍵データの正当性判定に応じてドアの開錠を実行するデバイスとする。あるいは、レンタカーの近傍に設置され、レンタカーの固定装置を前記正当性判定に応じて解除するデバイスであっても良い。

#### 【0 0 7 7】

また、ハードウェア構成および機能構成についても、第 1 の実施形態の場合（図 2、図 3 参照）とほぼ同様である。

#### 【0 0 7 8】

次に、本実施形態における電子鍵システムに用いられる各種のデータのデータ構成を、図 1 2 に示す。各種のデータのデータ構成は、第 1 の実施形態と同様な点は省略し、相違する点について次に説明する。

#### 【0 0 7 9】

電子鍵管理装置 3 0 0 の顧客テーブル 3 3 0 は、主 ID データと SD アドレスデータをデータ項目として有しない点で、第 1 の実施形態における顧客テーブル 3 3 0 と相違する。また、第 1 の実施形態では、利用者と、その利用者が利用するサービス提供デバイス（利用者の住宅のドアに取り付けられ電子鍵の正当性を判定するデバイス）は、あらかじめ固定されているため、主 ID は会員番号に 1 対 1 に対応して設定されていた（図 4 の顧客テーブル 3 3 0 参照）。しかしながら、本実施形態では、利用者と利用者が利用するレンタカーとの関係は、あらかじめ固定されていない。そのため、利用者がレンタカーを選択し、レンタカーの鍵を購入するタイミングで、利用者とレンタカーとを対応付ける必要がある。そのため、本実施形態の電子鍵管理装置 3 0 0 には、第 1 の実施形態にはない新たなテーブルとして、取引テーブル 3 4 0 および商品テーブル 3 5 0 を有する。

#### 【0 0 8 0】

取引テーブル 3 4 0 は、電子鍵の購入取引を管理するテーブルであり、個々の

電子鍵を識別するための主 I D、該主 I D の電子鍵に対応する商品を識別するための商品 I D、該主 I D の電子鍵の購入者を識別するための会員番号を有する。取引テーブル 3 4 0 は、利用者がレンタカーの鍵を購入するタイミングで、レコードが作成され、取引テーブルに追加さる。

#### 【 0 0 8 1 】

商品テーブル 3 5 0 は、サービス提供者が提供する商品を管理するテーブルであり、商品（本実施形態においてはレンタカー）を一意に識別する商品 I D、商品の名称を表す商品名、該商品と対応するサービス提供デバイス 4 0 0 のネットワークアドレスである S D アドレスを有する。

#### 【 0 0 8 2 】

なお、本実施形態において図 1 2 に示したテーブルおよびデータは、次の 4 つのテーブルを除き、各装置のメモリ 9 0 2 または外部記憶装置 9 0 3 にあらかじめ設定されているものとする。その 4 つのテーブルとは、利用者電子鍵テーブル 1 2 0、取引テーブル 3 4 0、サービス許可テーブル 4 3 0、サービス拒否テーブル 4 4 0 である。

#### 【 0 0 8 3 】

次に図 1 3 および図 1 4 を参照し、利用者が電子鍵を購入するときの処理の流れを説明する。図 1 3 は処理フロー図で、図 1 4 は利用者端末の表示画面例であり、本表示画面の例では、副 I D に携帯電話番号を使用している。なお、基本的に各メッセージの送受信、相互認証処理など、第 1 の実施形態と同様である。

#### 【 0 0 8 4 】

利用者端末 2 0 0 は「会員番号・パスワード入力画面」（画面 5 1）から入力された会員番号およびパスワードを電子鍵管理装置 4 0 0 に送信する（ステップ 5 0 1）。電子鍵管理装置 4 0 0 は、会員番号およびパスワードの入力を受信し、顧客テーブル 3 3 0 を参照してログイン処理を実行し、メニュー画面（画面 5 2）を利用者端末 2 0 0 に送信する（ステップ 5 0 2）。これらの処理は、第 1 の実施形態の無効化処理（図 1 0、図 1 1 参照）と同様である。ただし、メニューとして表示する内容は、画面 5 2（図 1 4）と画面 4 2（図 1 1）とで異なる。



**【 0 0 8 5 】**

次にメニュー画面（画面 5 2）において、「商品購入」メニューが選択された場合の処理の流れについて以下に説明する。なお、「無効登録」が選択された場合に実行される電子鍵無効化処理については後述する。

**【 0 0 8 6 】**

利用者端末の入力部 2 8 3 は、「商品購入」メニューの選択を受け付け、遠距離無線通信部 2 8 4 は選択メニューの情報を電子鍵管理装置に送信する（ステップ 5 0 3）。電子鍵管理装置 3 0 0 の通信部が該メッセージを受け付けると、制御部 3 8 1 は商品テーブル 3 5 0 を検索し、商品 I D データと商品名データのペアを複数個取得し、通信部 3 8 3 はこれを利用者端末 2 0 0 に送信する（ステップ 5 0 4）。利用者端末 2 0 0 の遠距離無線通信部 2 8 4 は、該データを受信し、表示部 2 8 5 は受信データに基づき商品一覧画面（画面 5 3）を出力装置 9 0 6 に表示し、利用者の商品選択の入力を受け付ける（ステップ 5 0 5）。その後、利用者端末 2 0 0 の入力部 2 8 3 が受け付けた商品の商品 I D データを、遠距離無線通信部 2 8 4 が電子鍵管理装置 3 0 0 に送信し、その後、出力装置 9 0 6 にダウンロード処理中画面（画面 5 4）が表示される。

**【 0 0 8 7 】**

電子鍵管理装置 3 0 0 の通信部 3 8 3 が該商品 I D データを受信した後に、制御部 3 8 1 は、利用者モジュール 1 0 0 と相互認証処理を実行する（ステップ 5 0 6）。認証鍵としては、電子鍵管理装置 3 0 0 の U M 認証鍵データ 3 1 1 と利用者モジュール 1 0 0 の U M 認証鍵データ 1 1 0 を使用する。

**【 0 0 8 8 】**

次に、電子鍵管理装置 3 0 0 の制御部 3 8 1 は、主 I D データと副 I D データの生成処理を行う（ステップ 5 0 7）。主 I D データとしては、他の発行済み電子鍵と区別するために、それらの電子鍵の主 I D データとは異なる一意のデータ値を用いる。例えば、電子鍵管理装置 3 0 0 においてシリアル番号を管理し、電子鍵の発行ごとにその値をカウントアップし、その値を用いることが考えられる。副 I D データには、発行した電子鍵を共有する利用者のグループ内で一意となるデータ値を設定すれば良く、本実施形態では利用者の携帯電話番号を使用する

**【0089】**

次に電子鍵管理装置300の制御部381は、鍵名称データ、主IDデータ、共有階層データ、副ID履歴データを有する電子鍵データを生成する（ステップ508）。鍵名称データには、ステップ505で受信した商品IDデータを検索キーとして特定された商品テーブル350の商品名データを設定する。主IDデータおよび副ID履歴データには、ステップ507で生成された主IDデータおよび副IDデータをそれぞれ設定する。共有階層データには、第1の実施形態と同様に、その電子鍵の共有可能な範囲を表す所定の数値データを設定する。そして、電子鍵管理装置300の制御部381は、取引テーブル340に今まで説明した主IDデータ、商品IDデータ、および会員番号データを有するレコードを新規に追加する。

**【0090】**

次に、電子鍵管理装置300の制御部381は、サービス提供デバイス400との間で相互認証処理を実行する（ステップ509）。認証鍵としては電子鍵管理装置300のSD認証鍵データ310およびサービス提供デバイス400のSD認証鍵データ410を使用する。通信対象とするサービス提供デバイス400のネットワークアドレスは、商品テーブル350における対応SDアドレスデータを設定する。該対応SDアドレスデータは、ステップ505で受信した商品IDデータを検索キーとして特定する。

**【0091】**

次に、電子鍵管理装置300の通信部383は、ステップ507で生成した主IDデータを含む登録要求メッセージを、サービス提供デバイス400に送信する（ステップ510）。

**【0092】**

サービス提供デバイス400の通信部483は、該登録要求メッセージを受信し、制御部はサービス許可テーブル430に受信した主IDデータを追加する（ステップ512）。

**【0093】**

次に、電子鍵管理装置 3 0 0 の通信部 3 8 3 は、ステップ 5 0 8 で生成した電子鍵データを含む電子鍵書込メッセージを、利用者端末 2 0 0 の UM 通信部 2 8 6 を経由して、利用者モジュール 1 0 0 に送信する（ステップ 5 1 1）。利用者モジュール 1 0 0 の UT 通信部 1 8 3 は電子鍵データを受信し、制御部 1 8 1 が該電子データを利用者電子鍵テーブル 1 2 0 に追加する（ステップ 5 1 3）。その後、利用者端末 2 0 0 の出力装置 9 0 6 には終了画面（画面 5 5）が表示される。

#### 【 0 0 9 4 】

以上により、利用者が電子鍵を購入するときの処理を終了する。本処理により、利用者があらかじめ固定されていない任意のサービス提供デバイスを利用する場合であっても、電子鍵を利用したサービスの提供（レンタカーの鍵の購入）を受けることが可能である。

#### 【 0 0 9 5 】

電子鍵利用処理および電子鍵共有処理については、第 1 の実施形態の場合（図 5、6、7 参照）と同様である。なお、電子鍵共有処理における利用者端末 2 0 0 の表示画面については、図 1 4 に示すとおりである。

#### 【 0 0 9 6 】

電子鍵無効化処理については、第 1 の実施形態の場合（図 1 0 参照）と以下の点で相違する。相互認証処理（ステップ 4 0 6）の通信対象とするサービス提供デバイス 4 0 0 のネットワークアドレスは、本実施形態においてはログイン処理（ステップ 5 0 2）で受信した会員番号データから特定した商品テーブル 3 5 0 の SD アドレスデータとする。具体的には、会員番号データを検索キーとして取引テーブル 3 4 0 から商品 ID を特定し、該商品 ID を検索キーとして商品テーブル 3 5 0 の SD アドレスデータを特定する。

#### 【 0 0 9 7 】

また、部分無効化処理（ステップ 4 0 8）および全体無効化処理（ステップ 4 1 0）で送信するメッセージに含まれる主 ID データは、ログイン処理（ステップ 4 0 2）で受信した会員番号データを検索キーとして取引テーブル 3 4 0 を検索し取得する。なお、電子鍵無効化処理における利用者端末 2 0 0 の表示画面に

については、図 1 4 に示すとおりである。

#### 【0 0 9 8】

以上により、本発明に係る第 2 の実施の形態について説明した。本処理により、利用者があらかじめ固定されていない任意のサービス提供デバイスを利用する場合であっても、第 1 の実施形態と同様に、同一の主 I D を有する利用者モジュールの全部を無効化する全体無効化処理だけでなく、該当する副 I D を有する利用者モジュールのみを無効化する部分無効化処理が可能である。

#### 【0 0 9 9】

以上説明したように本発明によれば、複数の利用者で電子鍵を共有してサービスを共同利用する場合において、盗難や紛失などの理由により誰かの電子鍵を無効化する場合でも、必ずしも全ての電子鍵を無効化する必要はなくなる。つまり、利用者の一人が電子鍵を紛失し（あるいは盗難され）、その電子鍵を無効化すると、その利用者と電子鍵を共有していた利用者の全員が必ずサービスの利用を拒否されるという事態を、防止することが可能となる。

#### 【0 1 0 0】

なお、本発明は上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。例えば、レンタル会議室の電子鍵、ホテルの部屋の電子鍵、電子ロッカーの電子鍵などがある。

#### 【0 1 0 1】

例えば、第 1 の実施の形態の利用処理においては、サービス提供デバイス 4 0 0 がサービス許可テーブル 4 3 0 およびサービス拒否テーブル 4 4 0 を有し、サービス提供可否の判断を行っている。しかしながら電子鍵管理装置 3 0 0 が、各サービス提供デバイス 4 0 0 のサービス許可テーブル 4 3 0 およびサービス拒否テーブル 4 4 0 を保持し、サービス提供可否の判断を行うこととしてもよい。具体的には、図 5 における電子鍵送信（ステップ 1 0 3）の送信先を、電子鍵管理装置 3 0 0 とし、電子鍵管理装置 3 0 0 がサービス提供可否判断（ステップ 1 0 4 ～ステップ 1 0 7）を行い、その判断結果をサービス提供デバイス 4 0 0 に送信することが考えられる。

#### 【0 1 0 2】

また、第 1 の実施の形態の共有処理においては、利用者モジュール 1 0 0 が利用者電子鍵テーブル 1 2 0 を有し、共有用電子鍵データを生成している。しかしながら、電子鍵管理装置 3 0 0 が、各利用者モジュールの利用者電子鍵テーブル 1 2 0 を保持し、一元管理して、利用者端末からの共有要求に応じて、共有用電子鍵データの生成をおこなうこととしてもよい。具体的には、図 7 における第 1 の利用者端末 2 0 0 の電子鍵一覧取得（ステップ 3 0 1）の送信先を、電子鍵管理装置 3 0 0 とし、それ以降の第 1 の利用者モジュール 1 0 0 の処理（電子鍵一覧応答、共有用電子鍵生成等）を電子鍵管理装置 3 0 0 が行うことが考えられる。

### 【0 1 0 3】

#### 【発明の効果】

以上のように、本発明によれば、複数の利用者で電子鍵を共有してサービスを共同利用することが可能となる。また、共有する電子鍵を無効にする場合に、全ての共有する電子鍵を無効にするだけでなく、一部の電子鍵のみを無効にすることが可能となる。

#### 【図面の簡単な説明】

- 【図 1】 本発明の第 1 の実施形態におけるシステム構成図。
- 【図 2】 本発明の第 1 の実施形態におけるハードウェア構成図。
- 【図 3】 本発明の第 1 の実施形態における機能構成図。
- 【図 4】 本発明の第 1 の実施形態におけるデータ構成図。
- 【図 5】 本発明の第 1 の実施形態における電子鍵利用処理のフロー図。
- 【図 6】 本発明の第 1 の実施形態における電子鍵利用処理のフロー図。
- 【図 7】 本発明の第 1 の実施形態における電子鍵共有処理のフロー図。
- 【図 8】 本発明の第 1 の実施形態における電子鍵共有時のデータ値の例。
- 【図 9】 本発明の第 1 の実施形態における電子鍵共有時のデータ値の例。
- 【図 1 0】 本発明の第 1 の実施形態における電子鍵無効化処理のフロー図。
- 【図 1 1】 本発明の第 1 の実施形態における画面表示例。
- 【図 1 2】 本発明の第 2 の実施形態におけるデータ構成図。
- 【図 1 3】 本発明の第 2 の実施形態における電子鍵購入処理のフロー図。
- 【図 1 4】 本発明の第 2 の実施形態における画面表示例。

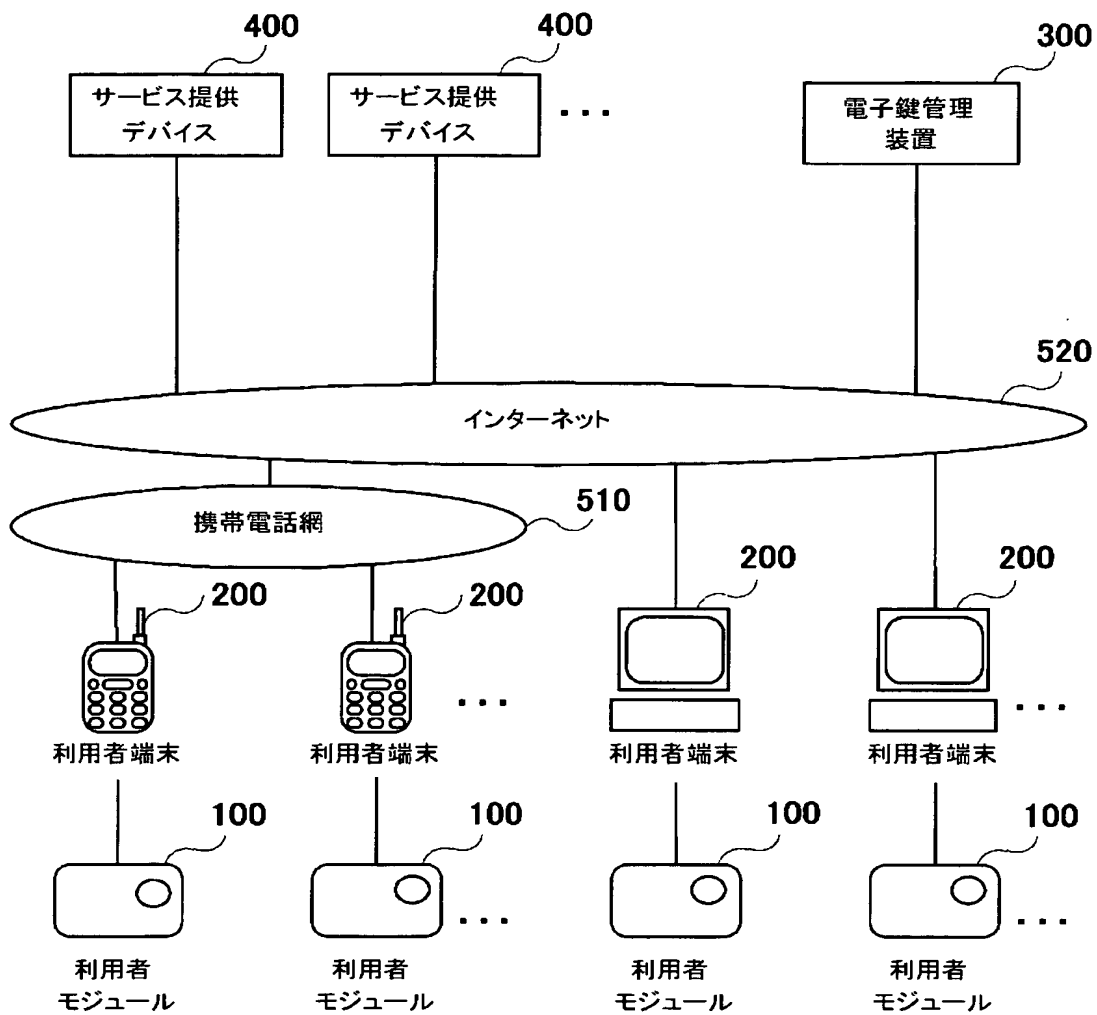
**【符号の説明】**

1 0 0 …利用者モジュール、1 1 0 …UM認証鍵データ、1 2 0 …利用者鍵テーブル、2 0 0 …利用者端末、3 0 0 …電子鍵管理装置、3 1 0 …SD認証鍵データ、3 2 0 …UM認証鍵データ、3 3 0 …顧客テーブル、4 0 0 …サービス提供デバイス、4 1 0 …SD認証鍵データ、4 2 0 …UM認証鍵データ、4 3 0 …サービス許可テーブル、4 4 0 …サービス拒否テーブル

【書類名】 図面

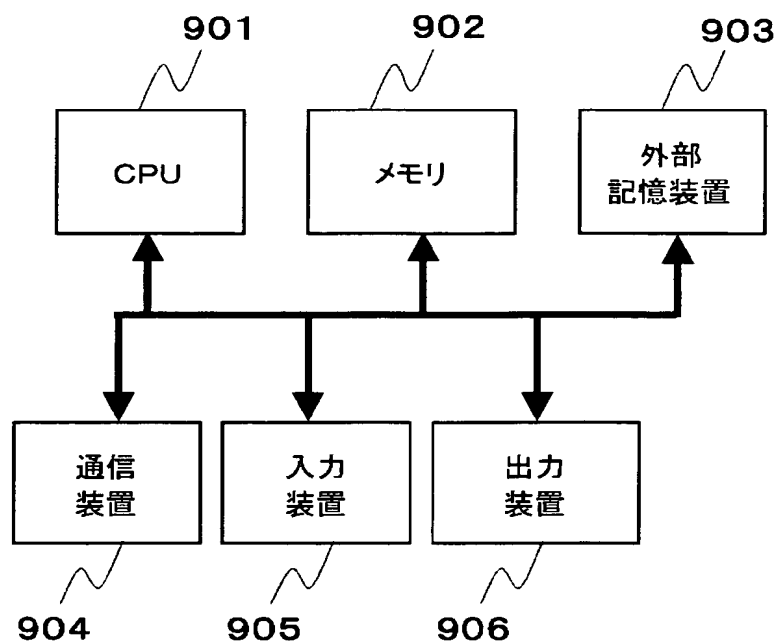
【図 1】

図 1



【図 2】

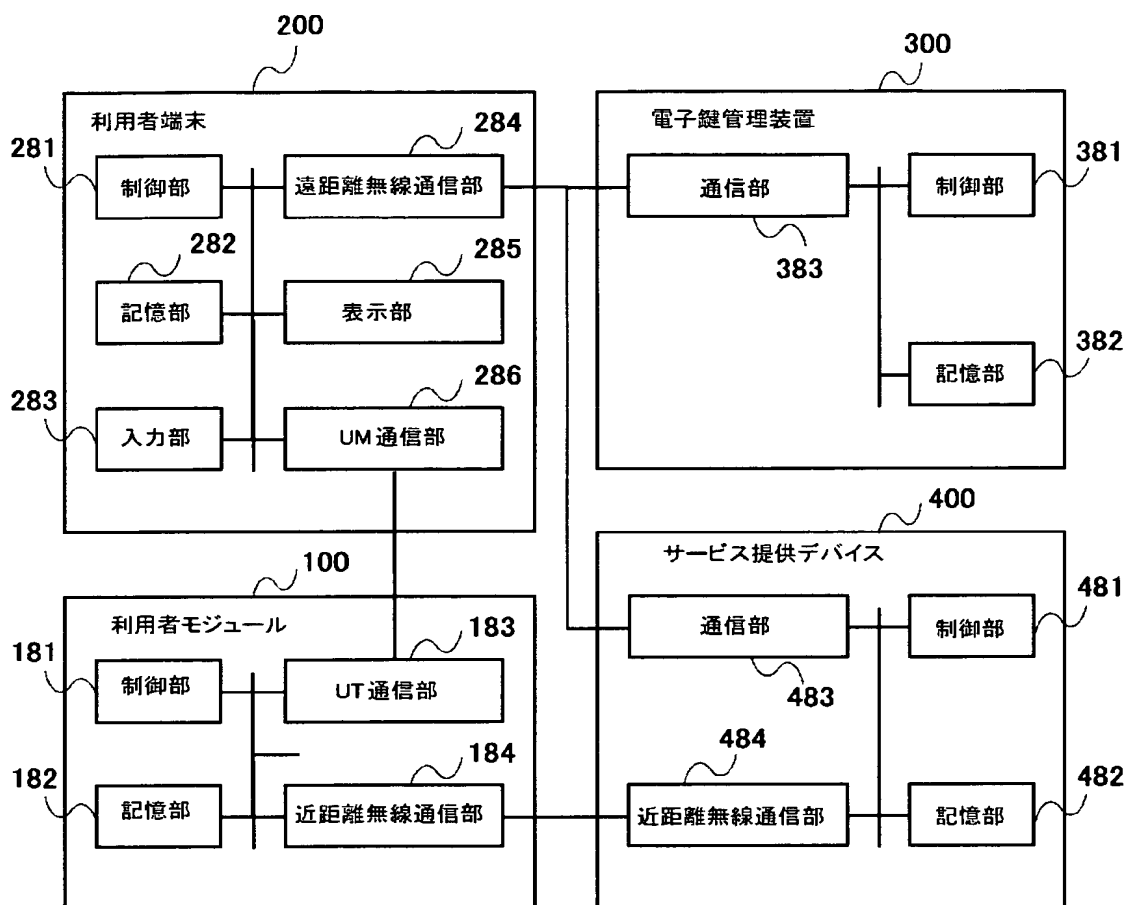
図2





【図 3】

図3



【図 4】

図 4

利用者モジュールのデータ

110  
UM 認証鍵データ

UM 認証鍵
Kauu

120  
利用者電子鍵テーブル

鍵名称	主 ID	共有階層	副 ID (携帯電話番号) 履歴
XX 宅	0120040101001	1	XXX-XXX-XXXX
⋮	⋮	⋮	⋮

電子鍵管理装置のデータ

310  
SD 認証鍵データ

SD 認証鍵
Kaus

320  
UM 認証鍵データ

UM 認証鍵
Kauu

330  
顧客テーブル

会員番号	パスワード	副 ID (携帯電話番号)	主 ID	SD アドレス
001	0001	XXX-XXX-XXXX	20040101001	XXX.XXX.XXX.XXX
002	0002	YYY-YYY-YYYY	20040101002	YYY.YYY.YYY.YYY
⋮	⋮	⋮	⋮	⋮

サービス提供デバイスのデータ

410  
SD 認証鍵データ

SD 認証鍵
Kaus

420  
UM 認証鍵データ

UM 認証鍵
Kauu

430  
サービス許可テーブル

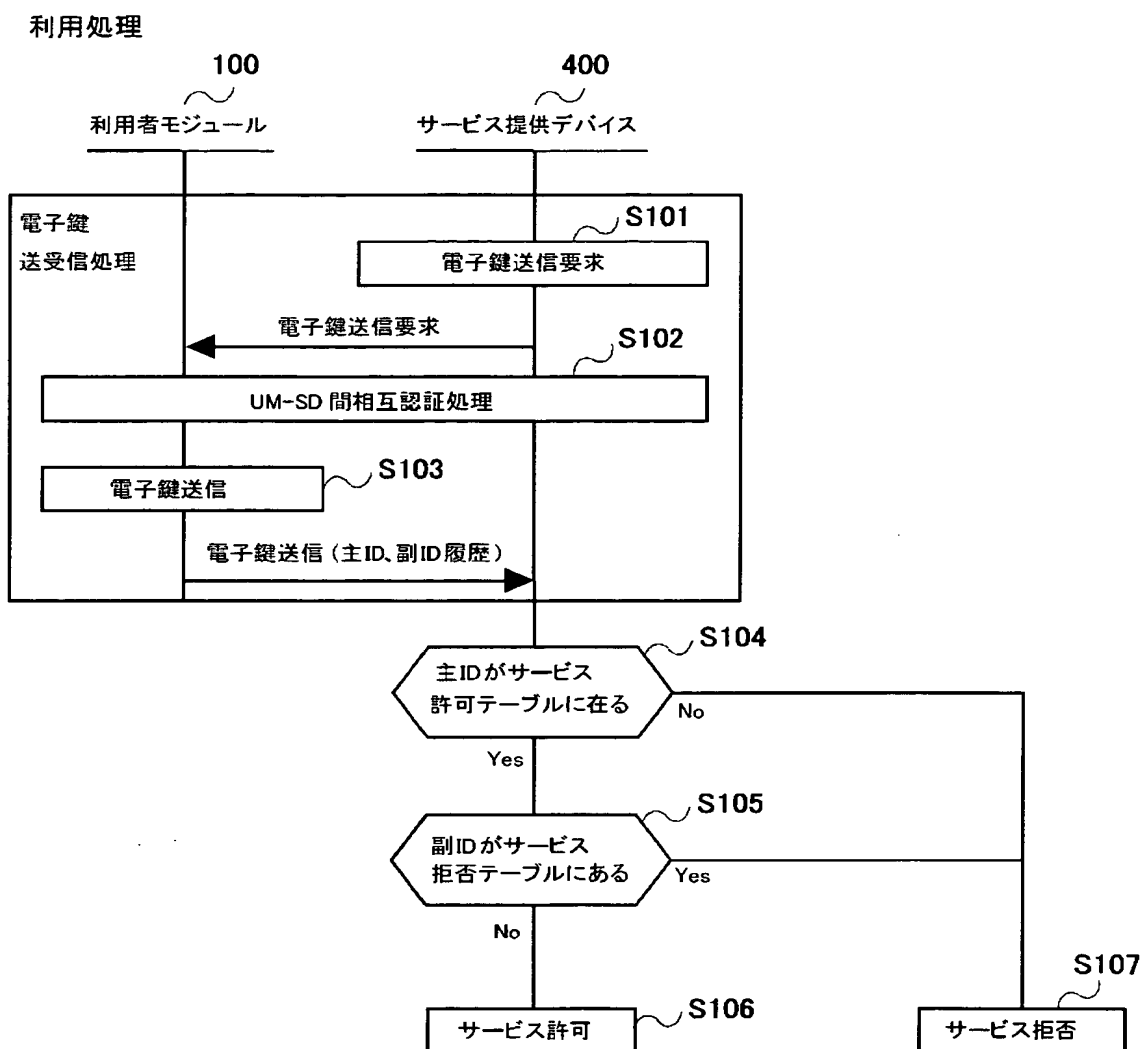
主 ID
0120040101001
0120040101002
⋮

440  
サービス拒否テーブル

主 ID	副 ID
0120040101001	ZZZ-ZZZ-ZZZZ
⋮	⋮

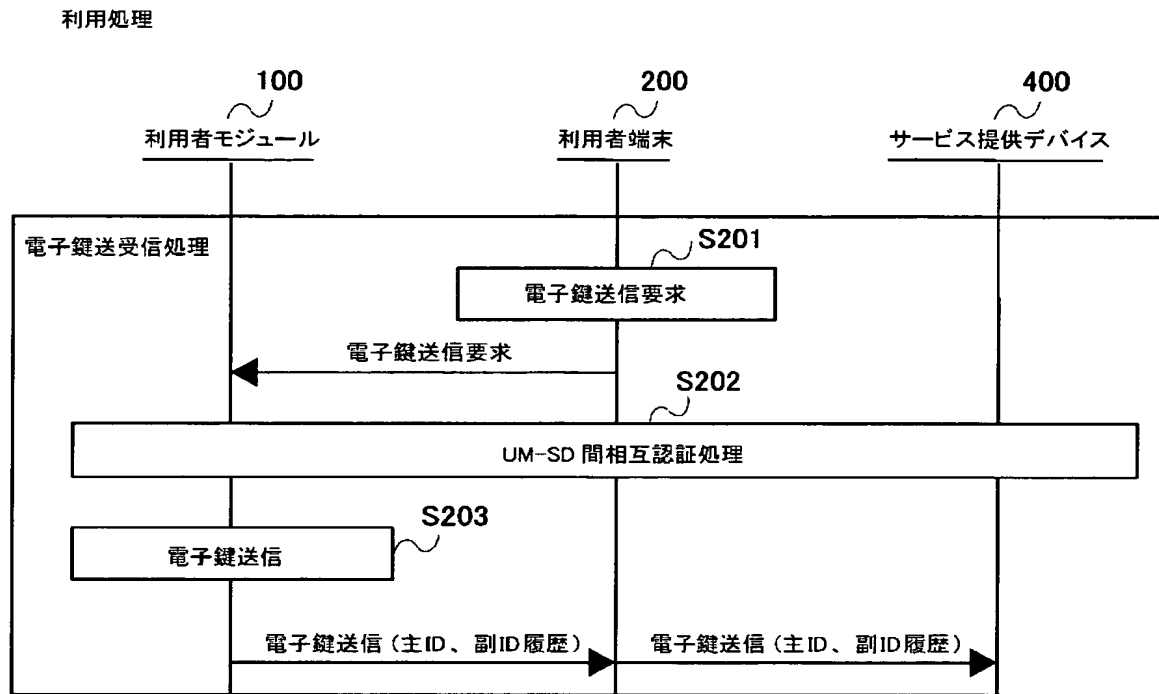
【図5】

図5



【図 6】

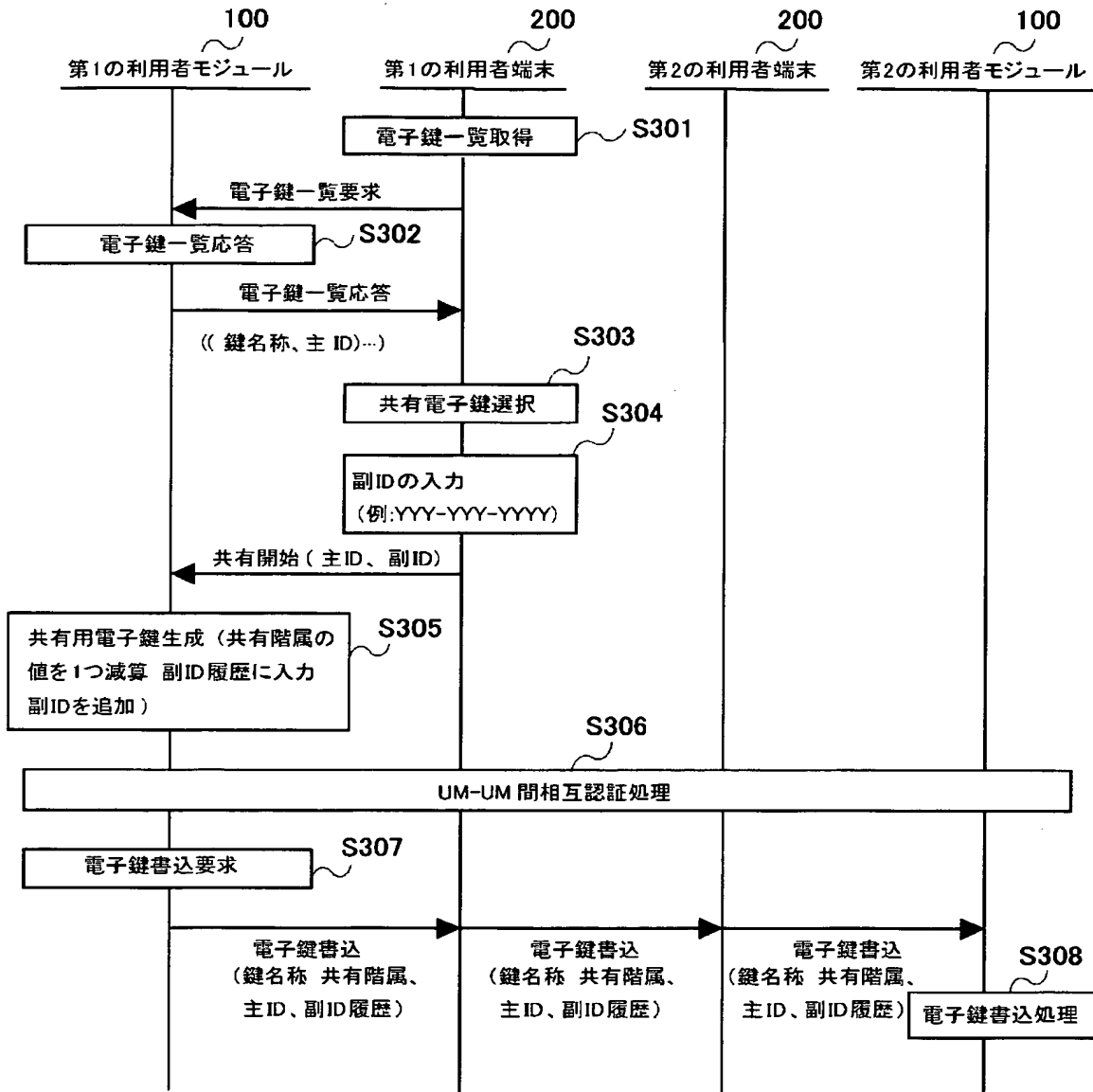
図6



【図 7】

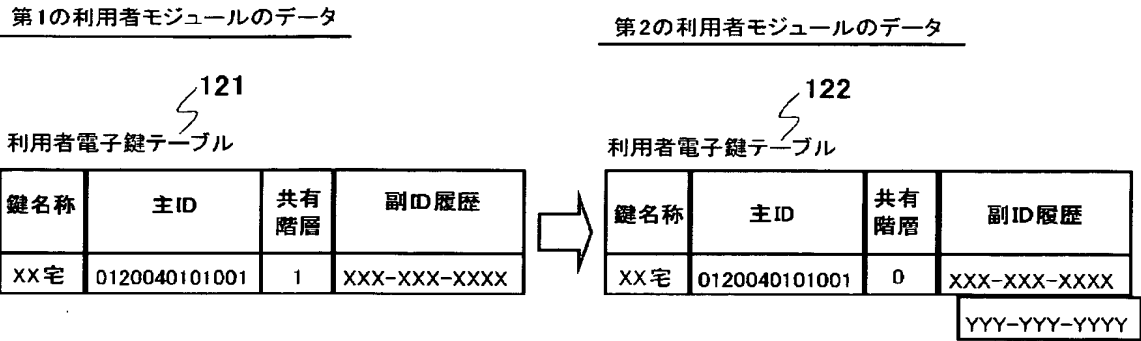
図 7

共有処理



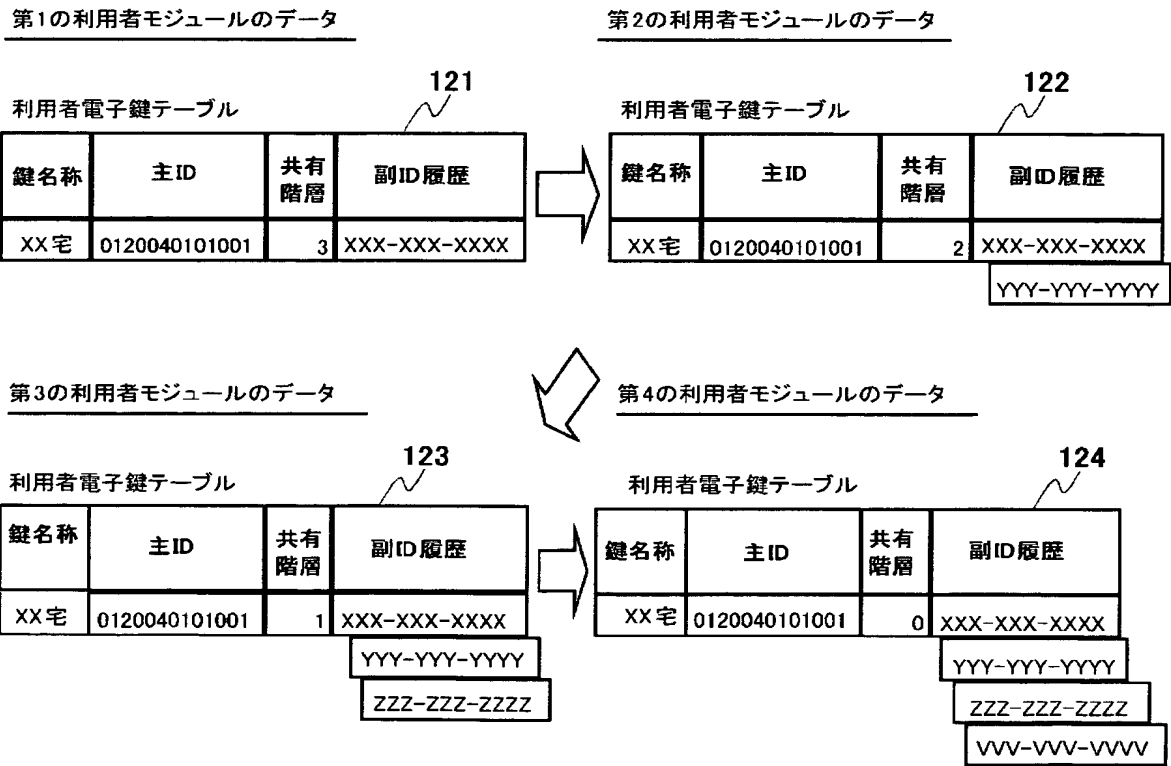
【図 8】

図 8



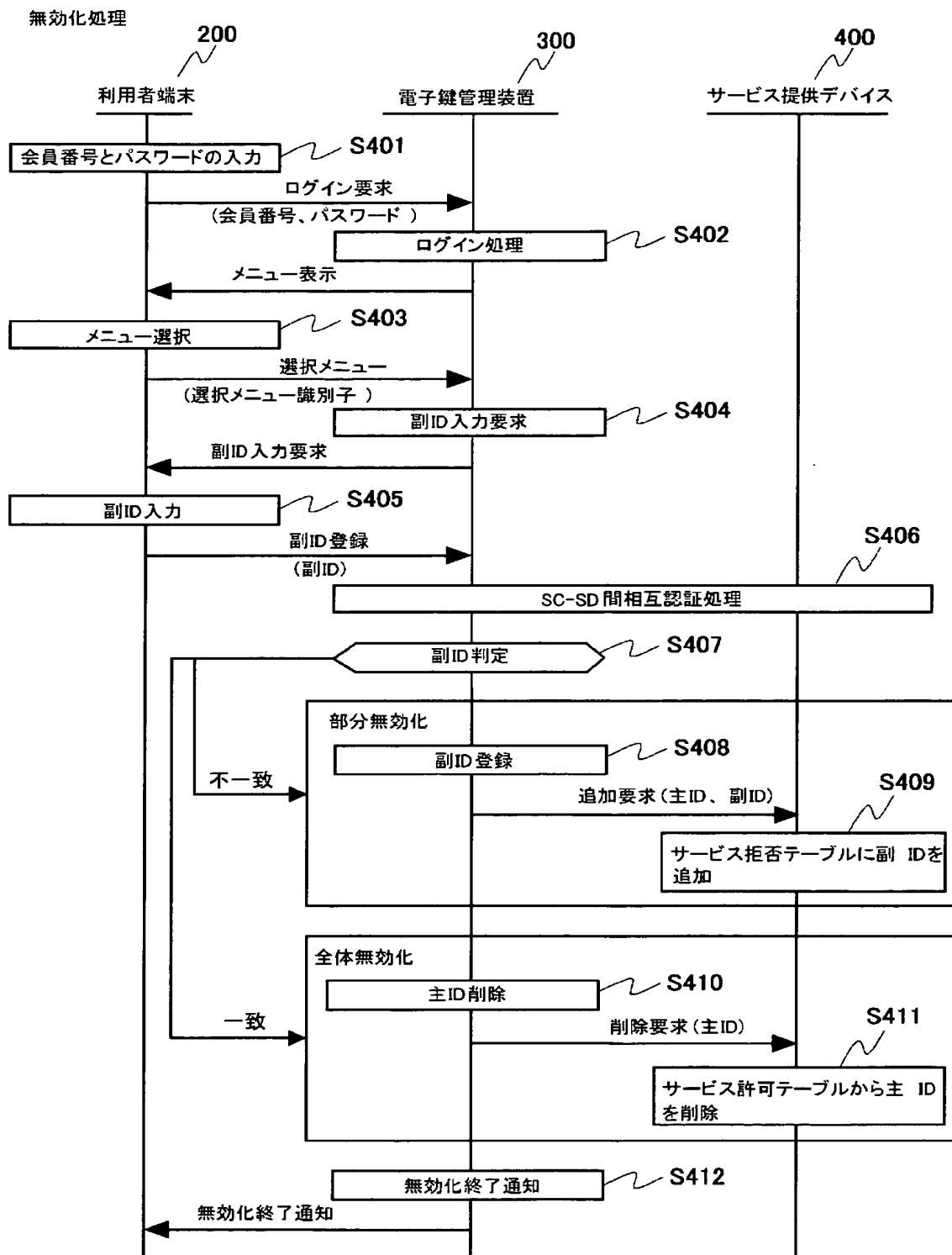
【図 9】

図 9



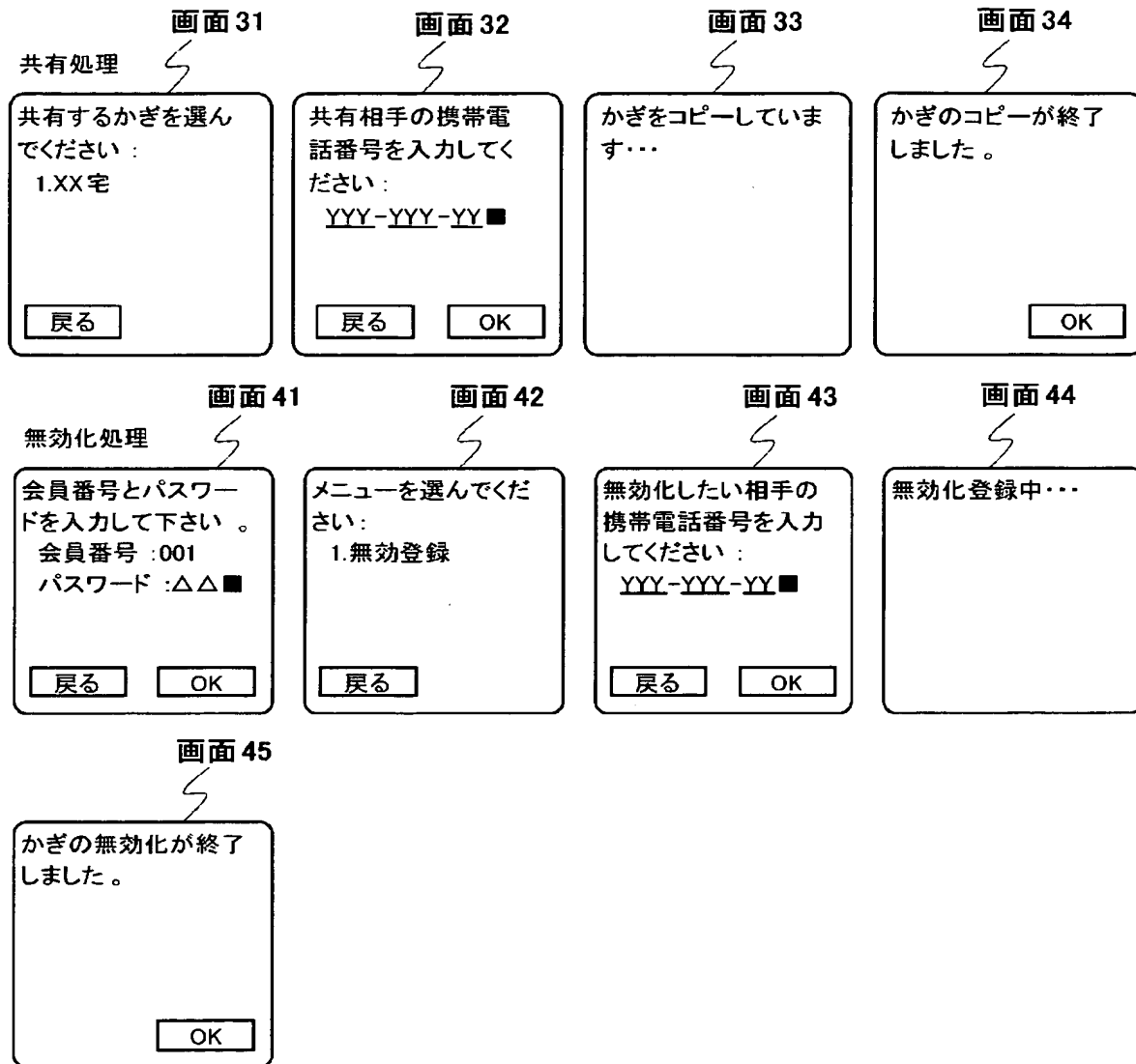
【図 10】

図 10



【図 11】

図 11





【図 12】

図 12

## 利用者モジュールのデータ

110

UM認証鍵データ

UM 認証鍵

Kauu

120

利用者電子鍵テーブル

鍵名称	主ID	共有階層	副ID (携帯電話番号)履歴
車種A	0120040101001	1	XXX-XXX-XXXX
車種B	0120040101002	0	YYY-YYY-YYYY
⋮	⋮	⋮	⋮

## 電子鍵管理装置のデータ

310

320

330

SD認証鍵データ

UM認証鍵データ

顧客テーブル

SD認証鍵
Kaus

UM認証鍵
Kauu

会員番号	パスワード	副ID (携帯電話番号)
001	0001	XXX-XXX-XXXX
002	0002	YYY-YYY-YYYY
⋮	⋮	⋮

340

350

取引テーブル

商品テーブル

主ID	商品ID	会員番号
0120040101001	001	001
0120040101002	002	002
⋮	⋮	⋮

商品ID	商品名	対応SDアドレス
001	車種A	XXX.XXX.XXX.X
002	車種B	YYY.YYY.YYY.Y
⋮	⋮	⋮

## サービス提供デバイスのデータ

410

SD 認証鍵データ

SD 認証鍵
Kaus

420

UM 認証鍵データ

UM 認証鍵
Kauu

430

サービス許可テーブル

主ID
0120040101001
0120040101002
⋮

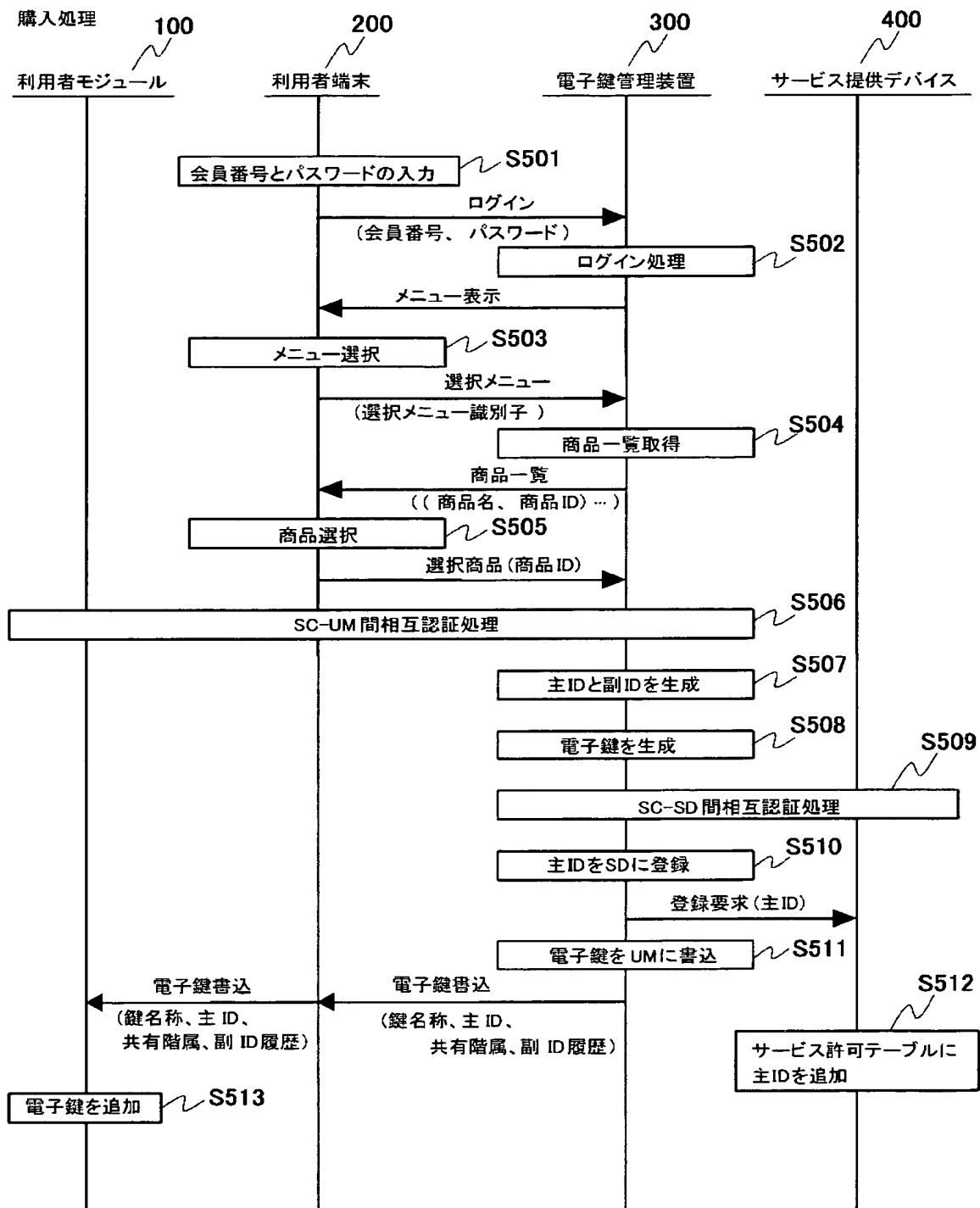
440

サービス拒否テーブル

主ID	副ID
0120040101001	ZZZ-ZZZ-ZZZZ
⋮	⋮

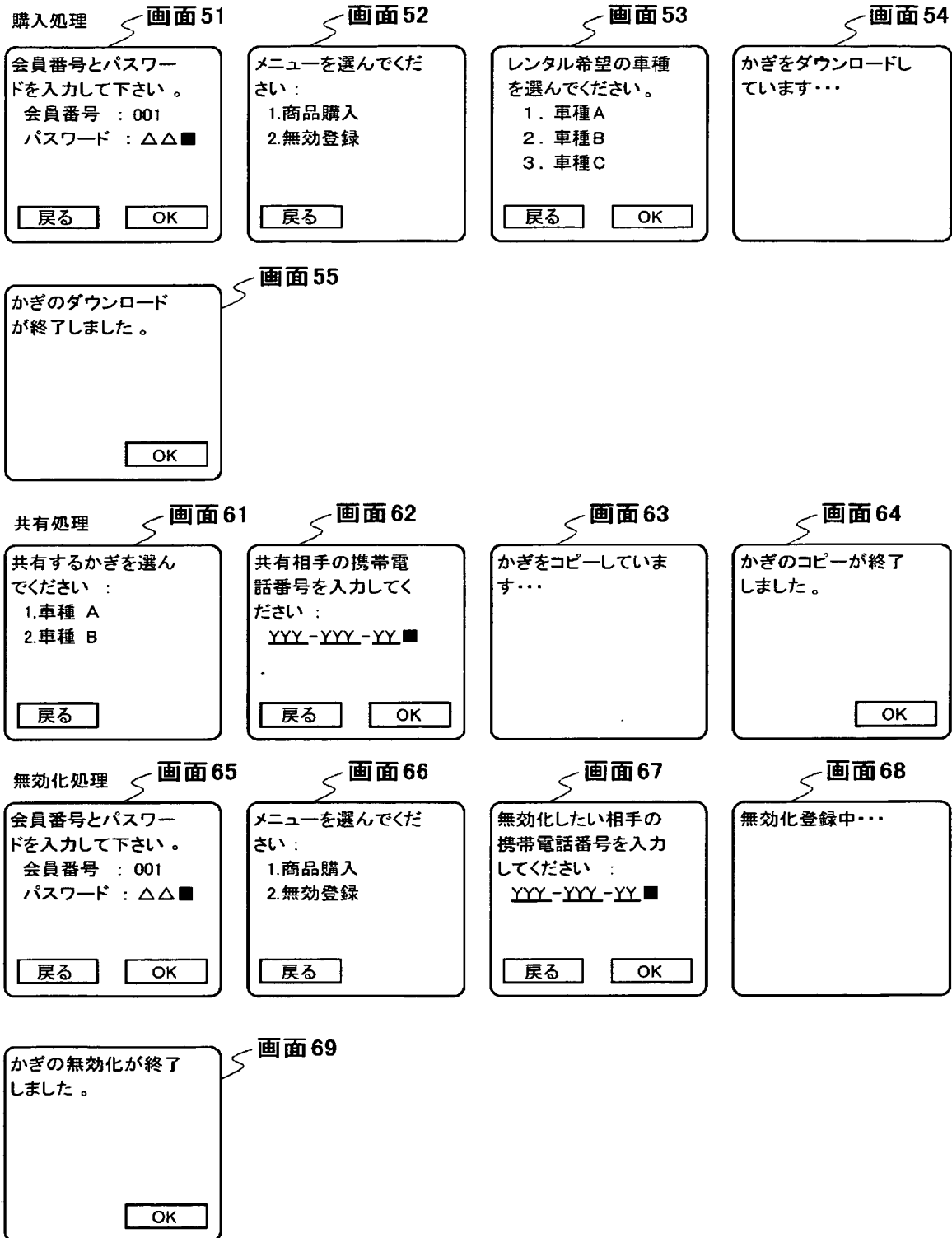
【図 13】

図 13



【図 1 4】

図 1 4



【書類名】 要約書

【要約】

【課題】複数の利用者で共有電子鍵によりサービスを共同利用する場合に、一部の人のみの電子鍵を無効化する方法を提供する。

【解決手段】利用者の保有する利用者モジュール100に格納する電子鍵データは、主IDデータと副ID履歴データの2つのデータを有する。サービス提供デバイス400は、サービス許可テーブルとサービス拒否テーブルの2つのテーブルを保持し、電子鍵データを利用者モジュール100から受信したときに、電子鍵の主IDデータがサービス許可テーブルに存在し（ステップ104）、かつ副ID履歴データに含まれる副IDデータがサービス拒否テーブルに存在しない場合のみ（ステップ105）、サービス利用を許可する（ステップ106）。

【選択図】 図5

特願 2003-118126

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所